

INSIDE: Securing Your Mobile Device • Preserving Social Media Content • How To Protect Sensitive Data

# Delaware Lawyer

A PUBLICATION OF THE  
DELAWARE BAR FOUNDATION



VOLUME 32 ♦ NUMBER 3  
\$3.00 ♦ FALL 2014

## THE TECHNOLOGY ISSUE



## Risks and Responsibilities In Managing Technology

Nonprofit Organization  
U.S. Postage  
PAID  
Wilmington, Delaware  
PERMIT NO. 697



## YOU RECOGNIZE A CLASSIC WHEN YOU SEE IT


One of the nation's most highly acclaimed antiques shows presents a spectacular showcase of art, antiques, and design! Featuring the finest offerings from more than 60 distinguished dealers, the Delaware Antiques Show highlights the best of American antiques and decorative arts. Join us for a full schedule of exciting show features sure to captivate the sophisticated and new collector alike.

### OPENING NIGHT PARTY

Thursday, November 6 • 5:00–9:00 pm

Celebrate the opening of the show with cocktails and exclusive early shopping!

*(Opening Night Party requires a separate ticket, which includes admission for all three days.)*

Opening Night Party made possible by  WILMINGTON TRUST

### SHOW TICKETS ON SALE NOW!

November 7–9, 2014

Chase Center on the Riverfront  
Wilmington, Delaware

*Benefits Educational Programming at Winterthur*

Tickets: \$15 per person; \$13 per Member; children under 12 free. Tickets valid for all days of the show. For tickets call 800.448.3883 or visit [winterthur.org/das](http://winterthur.org/das).

ENJOY TAX-FREE SHOPPING

### SPECIAL LECTURES

**Jessica Fellowes**

Friday, November 7, 10:00 am

Join Jessica Fellowes—author, historian, and niece of *Downton Abbey* creator Julian Fellowes—for a special talk focused on the award-winning television show. *Book signing to follow lecture.* \$30 per Member; \$35 per nonmember. For tickets call 800.448.3883. Includes admission to all three days of show.

Sponsored by DelawareToday. [MAINLINE TODAY](http://MainLineToday.com)

**Philip D. Zimmerman**

Museum and Decorative Arts Consultant

Saturday, November 8, 2:00 pm

*Historic Odessa: New Findings in an Old Collection\**

**Linda Eaton**

John L. & Marjorie P. McGraw Director of Collections and  
Senior Curator of Textiles at Winterthur

Sunday, November 9, 2:00 pm

*Patterns of Their Time: Design in Printed Textiles\**

Weekend lectures sponsored by THE HUNT

*\*Lectures included with general admission*

For tickets to the show or party or for more information, please call 800.448.3883 or visit [winterthur.org/das](http://winterthur.org/das).



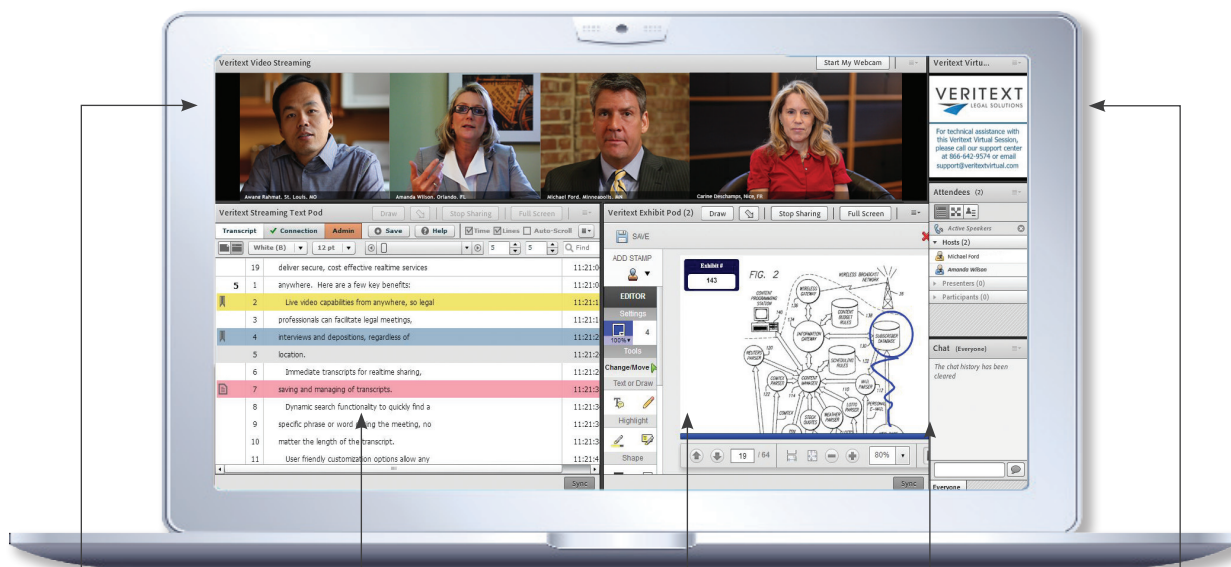
# Veritext Virtual 2.0

## Remote Depositions

(Now with enhanced annotation features  
for exhibits and streaming text!)

Proud  
Sponsor  
of the

2014  
Campaign  
for Justice



### Streaming Video

Realtime video lets you view witness demeanor and body language. Accommodates up to 100 participants.

### Streaming Text

Scrolling text of deposition can be highlighted, annotated and saved, without the need for additional software.

### Exhibit Sharing

Securely view, share, annotate and digitally stamp exhibits. Easily delegate control to other participants.

### Chat Feature

Engage in side conversations with other participants.

### Technical Support

24/7 technical support assists you with participating wherever there is an Internet connection.

Watch it in action at: [veritext.com/veritext-virtual](http://veritext.com/veritext-virtual)



300 Delaware Ave., Suite 815 | Wilmington, DE 19801

1111 B South Governors Ave. | Dover, DE 19901

Phone: 302.571.0510 Fax: 302.571.1321 | [www.veritext.com](http://www.veritext.com)

# Delaware Lawyer

CONTENTS



FALL 2014



On the Cover: The Commission on Law & Technology.

Cover and Contributors artwork by Commissioner Mark S. Vavala.  
Project Management by Chris Mourse

**EDITORS' NOTE** 6

**CONTRIBUTORS** 8

**FEATURES** 10 "Please Allow [Us] to Introduce Ourselves":  
The Commission on Law & Technology  
View from the Bench Working Group

16 Technology Competence for Lawyers:  
Not an Oxymoron  
Bruce E. Jameson

20 Securing Your Mobile Device  
Steven L. Butler

26 Managing Clients' Social-Media Evidence  
Margaret (Molly) DiBianca

30 The Data Security Imperative for Lawyers  
Edward J. McAndrew

36 **OF COUNSEL:** Justice Henry duPont Ridgely  
Kevin Brady & Richard Herrmann

## Experience + Integrity

Experience is the Difference®



Attorneys have turned to Gunnip  
for accounting services since 1947.

**Gunnip & company** LLP  
Certified Public Accountants and Consultants

302.225.5000  
[WWW.GUNNIP.COM](http://WWW.GUNNIP.COM)

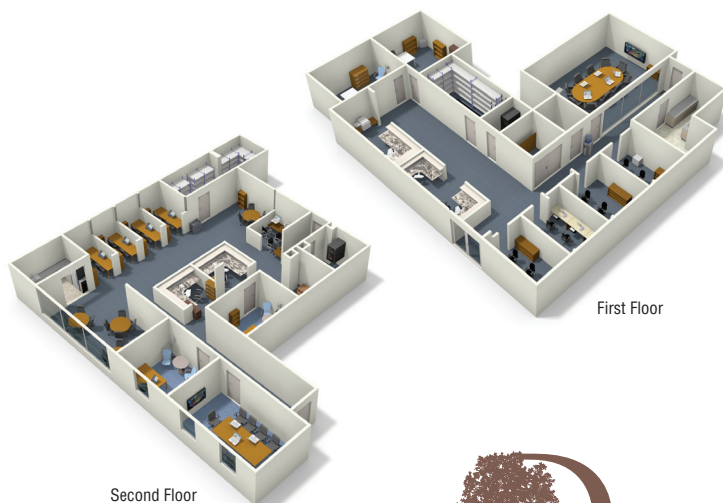




# DoubleTree by Hilton Downtown Wilmington Legal District

Now featuring 2 fully functional law centers located within one block of both the Federal and Superior Courthouses. Our 2 turnkey centers exceed 3,000 square feet in size and incorporate all of the following features:

- \* 2 private lead attorney offices
- \* Large War Room space with 52" HD flat screens
- \* 3 large administrative workstations
- \* 4 paralegal workstations accommodating up to 8 people
- \* Oversized file storage rooms complete with shelving
- \* Kitchen areas complete with full-size refrigerator, microwave, coffee maker and water cooler
- \* Direct-dial speakerphones with voicemail at each workstation
- \* Private, secured entrances with key card access
- \* 50 MG dedicated Internet service in each center
- \* Dedicated IT locations in each center



## For all your trial team needs contact:

Julie Shaw  
302.661.4316  
Julie.Shaw@Hilton.com



*\* Hilton Honors points signing bonus for trial teams in 2015! Ask for details!*

  
**DOUBLETREE**  
BY HILTON™  
DOWNTOWN WILMINGTON  
LEGAL DISTRICT

©2009 Hilton Hotels Corporation

700 North King Street • Wilmington, DE 19801  
Reservations: 1.800.222.TREE Hotel Direct: 302.655.0400  
[www.wilmingtonlegalcenter.com](http://www.wilmingtonlegalcenter.com)





## Action Plans are Better when Shared

Sheraton is where colleagues gather. Bring the best minds together in our full-service legal suites and war room space. Special legal packages with meals included help your team meet their full potential.



Three Full-Service Legal Suites can accommodate your special needs.



[Sheraton.com/suiteswilmington](http://Sheraton.com/suiteswilmington)

spg.  
Starwood  
Preferred  
Guest

422 Delaware Avenue | Wilmington, DE 19801  
tel: 302.654.8300 | fax: 302.576.8010

©2010 Starwood Hotels & Resorts Worldwide, Inc.  
All Rights Reserved. Sheraton and its logo are the trademarks of Starwood Hotels & Resorts Worldwide, Inc., or its affiliates.

# Delaware Lawyer

*A publication of Delaware Bar Foundation  
Volume 32 Number 3*

## BOARD OF EDITORS

*Chair:* Charles J. Durante

*Managing Editor:* Jacqueline Paradee Mette

Hon. Thomas L. Ambro  
Lawrence S. Drexler  
Dominick T. Gattuso  
Gregory A. Inskip  
Rosemary K. Killian  
James H.S. Levine  
Richard A. Levine  
David C. McBride  
Susan F. Paikin  
Karen L. Pascale  
Blake Rohrbacher  
Jeffrey M. Schlerf  
Kristine M. Wellman  
Gregory W. Werkheiser  
Robert W. Whetzel  
Hon. Loretta M. Young

## DELAWARE BAR FOUNDATION

100 W. 10th Street / Suite 106  
Wilmington, DE 19801  
302-658-0773 / 302-658-0774 (fax)

## BOARD OF DIRECTORS

*President:*

William H. Sudell, Jr.

Crystal Carey

Ryan Cicoski

Geoffrey Gamble

Hon. Randy J. Holland

Kathi A. Karsnitz

Elizabeth M. McGeever

Jenness E. Parker

David N. Rutt

Benjamin Strauss

Thomas P. Sweeney

E. Norman Veasey

*Executive Director:*

Melissa W. Flynn

## DELAWARE LAWYER

*is produced for the*

*Delaware Bar Foundation by:*

Today Media Custom Communications

3301 Lancaster Pike, Suite 5C

Wilmington, DE 19805

*Chairman:* Robert Martinelli

*President/Editor:* Jonathan Witty

*Art Director:* Samantha Carol Smith

*Subscriptions orders and address changes, call:*

Deanna Garrett, 302-656-1809

*Advertising information, call:*

Jessica Stryker, 302-504-1365

[jessica.stryker@todaymediacustom.com](mailto:jessica.stryker@todaymediacustom.com)

*Delaware Lawyer* is published by the Delaware Bar Foundation as part of its commitment to publish and distribute addresses, reports, treatises and other literary works on legal subjects of general interest to Delaware judges, lawyers and the community at large. As it is one of the objectives of *Delaware Lawyer* to be a forum for the free expression and interchange of ideas, the opinions and positions stated in signed material are those of the authors and not, by the fact of publication, necessarily those of the Delaware Bar Foundation or *Delaware Lawyer*. All manuscripts are carefully considered by the Board of Editors. Material accepted for publication becomes the property of Delaware Bar Foundation. Contributing authors are requested and expected to disclose any financial, economic or professional interests or affiliations that may have influenced positions taken or advocated in the articles. That they have done so is an implied representation by each author.

*Copyright 2014 Delaware Bar Foundation  
All rights reserved, ISSN 0735-6595*

# SMALL DETAILS INSPIRE BIG IDEAS

Our 2,100-square-foot legal center is a refreshing space designed to inspire productivity. The Westin Wilmington is home to the premier legal center in the area featuring:

- Large boardroom, corner offices and flexible workstations
- A private hospitality room and large refrigerator helps keep your team energized and focused
- Dedicated secured internet service, plus printer and copier access
- The legal center is accessible via key card only, and is available to your team 24 hours a day

With a state of the art full service Legal Center, healthy catered menus, and competitive room rates, you'll see what a pleasure it is to do business here.

FOR MORE INFORMATION OR TO SETUP A PERSONAL TOUR  
PLEASE CALL 302-654-2900



**THE WESTIN**  
WILMINGTON

spg<sup>\*</sup>  
Starwood  
Preferred  
Guest

MERIDIEN

aloft

FOUR  
POINTS

WESTIN

THE LUXURY  
COLLECTION

W  
HOTELS

Sheraton

ST REGIS

element



## EDITORS' NOTE

Kevin Brady & Richard Herrmann

Technology has made life simpler and more complex at the same time. It seems as if everyone has a smartphone and if you want the answer to just about any question, you can "Google" it. Information is available 24/7 and many of us are expected to be available, as well.

Advances in technology in the business world have occurred at breakneck speed over the last 20 years. Yet changes in technology in the legal community have occurred at a much slower pace, which creates a dilemma. Lawyers are trained to be risk averse. That is why clients want a lawyer's advice – in order to understand the benefits and risks associated with a certain task or issue.

Lawyers use case law and legal precedent to guide a client's future moves. If you look at the tools lawyers use to gather documents or information to litigate cases – complaints, answers, written discovery requests and depositions – they have not changed much in the past 25 years. While the volume of information that is relevant to the discovery process expanded exponentially during that same time period due to the use of technology, lawyers still considered themselves to be providing competent legal representation. Two years ago, that changed.

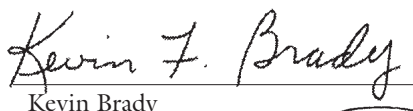
In August 2012, the House of Delegates of the American Bar Association approved changes to the ABA's Model Rules of Professional Conduct. In particular, the commentary to Rule 1.1 (Competence) was changed to require lawyers to understand the benefits and risks associated with technology that are relevant to their law practice. While on its face, that change does not seem to be that significant, a closer look will reveal the challenges that are inherent in understanding the benefits and risks associated with technology that is changing so quickly.

Where do you start? What questions do I ask? How much do you need to know to be considered "competent"? Do I really need to understand metadata, backup tapes, servers, databases and the "cloud"? If you feel this way you are not alone.

While many states which follow the Model Rules are adopting the changes promulgated by the ABA, Delaware, under the guidance of Justice Henry duPont Ridgely of the Delaware Supreme Court, has had the foresight to look for a practical way to provide guidance to all Delaware lawyers on the complexities that arise at the interface between law, technology and legal ethics. In July 2013, the Delaware Supreme Court formed the Delaware Commission on Law & Technology as a vehicle to provide ethical guidance regarding complex technology issues and to keep Delaware lawyers abreast of the changes in relevant technology.

What follows in this edition of *Delaware Lawyer* is a snapshot of the Commission's work and related information we hope will be of value to every member of the Delaware Bar.

AND WE would also like thank Commissioner Mark S. Vavala for creating the artwork for this issue. He has become an institution in the Delaware legal community for making people smile.

  
Kevin Brady

  
Richard Herrmann



## It's Time to Join or Renew Your Membership to the Delaware Bar Foundation!

*Not only does the Delaware Bar Foundation manages the IOLTA program for the Delaware Supreme Court which has provided over \$25million in the past 30 years to legal service for those less fortunate, but the Foundation also supports a variety of programs in our community such as:*

- Partnering with the University of Delaware on an in school anti-bullying program
- Creating a legal mentoring program for youth interested in careers in the field of law
- Publishing and providing Delaware Lawyer magazine free to every member of the Delaware Bar
- Supporting Liberty Day – Constitutional lessons for every fifth grade student in the Delaware Public Schools
- Sponsorship of the Mural Project by foster children in both the New Castle and Kent County Family Courts
- Funding the Senior Lawyer Oral History Project to compile personal recollections of Delaware legal history
- Sponsoring with the Delaware State Bar Association the Office and Trial Practice Seminar on October 29, 2014 at the Chase Center on the Riverfront
- Developing a student oriented, anti-bullying website, [www.DEleteBullying.org](http://www.DEleteBullying.org)

The Delaware Bar Foundation cannot continue this important work without your support.

To join, please see our website [www.DelawareBarFoundation.org](http://www.DelawareBarFoundation.org) and click the DONATE button. Thank you!

*All gifts are tax-deductible in accordance with IRS regulations.*



Redgrave LLP Welcomes

**KEVIN F. BRADY**

Nationally Recognized Leader in  
Technology and the Law to Our Firm

And Congratulates Kevin on his  
Co-Editorship of Delaware Lawyer's "Technology" Issue

---

**REDGRAVE LLP**

Focused on eDiscovery, Information Governance, Data Privacy and Data Security



**REDGRAVE LLP**  
INFORMATION MATTERS®

[WWW.REDGRAVELLP.COM](http://WWW.REDGRAVELLP.COM)

WASHINGTON DC



NORTHERN VIRGINIA



MINNEAPOLIS



SAN FRANCISCO

LIKE A GOOD WINE, KRESTON'S  
HAS THE BENEFIT OF AGE

*Celebrating 81 Years*



BEST  
WINE STORE

**KRESTON**  
WINE & SPIRITS

**Same Family, 4 Generations, Since 1933**  
Best Service. Best Selection. Best Price.

904 Concord Ave. (Concord & Broom)  
Mon-Sat 9-9 • Sun 12-4  
**302.652-3792**

Middletown Crossing Shopping  
Center Mon-Sat 9-9 • Sun 12-6  
**302.376-6123**

## CONTRIBUTORS

### The Jurists



#### Judge Kenneth S. Clark, Jr.

became a Judge for the Court of Common Pleas on April 28, 2000. After practicing law in Los Angeles, he returned to his native Delaware, where he practiced law in Sussex County for 15 years. Judge Clark is a graduate of Swarthmore College and received his J.D. from the University of California Hastings College of the Law.

#### Judge Eric M. Davis

became a Judge of the Superior Court on December 21, 2012. Prior to this appointment, he served for more than two years on the Court of Common Pleas. Judge Davis is a graduate of the University of Virginia and received his J.D. from the Emory University School of Law.

#### Judge Michael K. Newell

became a Judge of the Family Court on October 26, 2004. Previously, he spent more than 20 years practicing family law in Delaware. Judge Newell is a graduate of the University of Delaware. He received a Master's Degree from Northeastern University and his J.D. from the Widener University School of Law.

#### Vice Chancellor

##### Donald F. Parsons, Jr.

became a Vice Chancellor of the Court of Chancery on October 22, 2003. Previously, he spent more than 24 years in private practice, specializing in intellectual property litigation. He is a graduate of Lehigh University and received his J.D. from the Georgetown University Law Center.

#### Justice Henry duPont Ridgely

became a Justice on the Supreme Court on July 22, 2004. For the prior 20 years, he served as a general jurisdiction trial judge on the Superior Court and was the court's President Judge from 1990 until 2004. He is a graduate of Syracuse University, received his J.D. from the Catholic University of America Columbus School of Law and his L.L.M. in Corporate Law from George Washington University Law School.



**We Take You Where You Want to GO**

**Safe, Reliable, Convenient, Dependable and Affordable**

AIRPORT SHUTTLE • TOWN CAR SERVICE • CHARTER BUS SERVICE • DESTINATION GROUP TRAVEL



www.DelExpress.com Go AirportShuttle.com

# DELAWARE EXPRESS

Trusted Drivers Serving Your Business & Family Travel Since 1984

Celebrating 30 Years Driven By Excellence

(302) 484-7800 • 800-648-5466

DelExpress.com

"Like Us" to receive special offers.





## The Writers



### Kevin F. Brady

is Of Counsel to Redgrave LLP, one of the only law firms in the world focused exclusively on addressing complex legal challenges that arise at the intersection of the law and technology, especially in the areas of eDiscovery, information governance, data privacy, and data security matters. Kevin is Co-Chair of the Delaware Supreme Court's Commission on Law & Technology and President of the Richard K. Herrmann Technology American Inn of Court.

### Steven L. Butler

is a partner at Linarducci & Butler, PA in New Castle and focuses his practice on representing individuals for Social Security Disability claims. He works in a nearly-paperless environment and routinely uses his mobile devices while preparing claims and presenting to colleagues. He is a contributor to the iPlug Delaware blog (<http://www.iPlugDelaware.com>), and publishes blogs on Social Security Disability Law (<http://DelawareDisability.com/blog/>) and Mobile Technology for the Law Office (<http://Mobile4Law.com>). Mr. Butler is a member of the Delaware Supreme Court Commission on Law and Technology where he focuses on Mobile Computing.

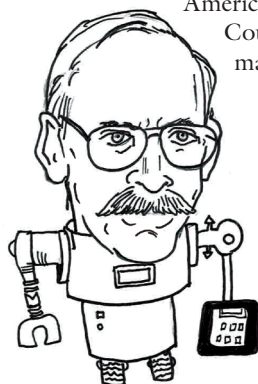


### Margaret (Molly) DiBianca

is an attorney with the law firm of Young Conaway Stargatt & Taylor, LLP, in Wilmington where she dedicates her legal practice to assisting employers as both a counselor and a litigator. She defends employers against claims brought by former and current employees and represents employers in their enforcement of restrictive covenants. She speaks regularly around the country, teaching best practices to human-resource professionals, executives and in-house counsel. Ms. DiBianca is the editor and primary contributor of the award-winning Delaware Employment Law Blog, which has been named one of the Top 100 Blogs in the country for four consecutive years and, in 2012, was named the Best Employment Law Blog in the country by the *ABA Journal*.

### Richard K. Herrmann

is a partner in the firm of Morris James LLP. He is Co-Chair of the Delaware Supreme Court's Commission on Law and Technology and serves on the Executive Committee of the Richard K. Herrmann Technology Inn of Court. He teaches eDiscovery, Technology and Ethics, and Law and Technology as Visiting Professor at Widener University School of Law, and Mobile Technology for the National Judicial College. He chairs the Delaware iPad Lawyer User Groups and authors technology columns for the *Delaware Bar Journal* and the American Inns of Court's *The Benchers* magazine.



### Bruce E. Jameson

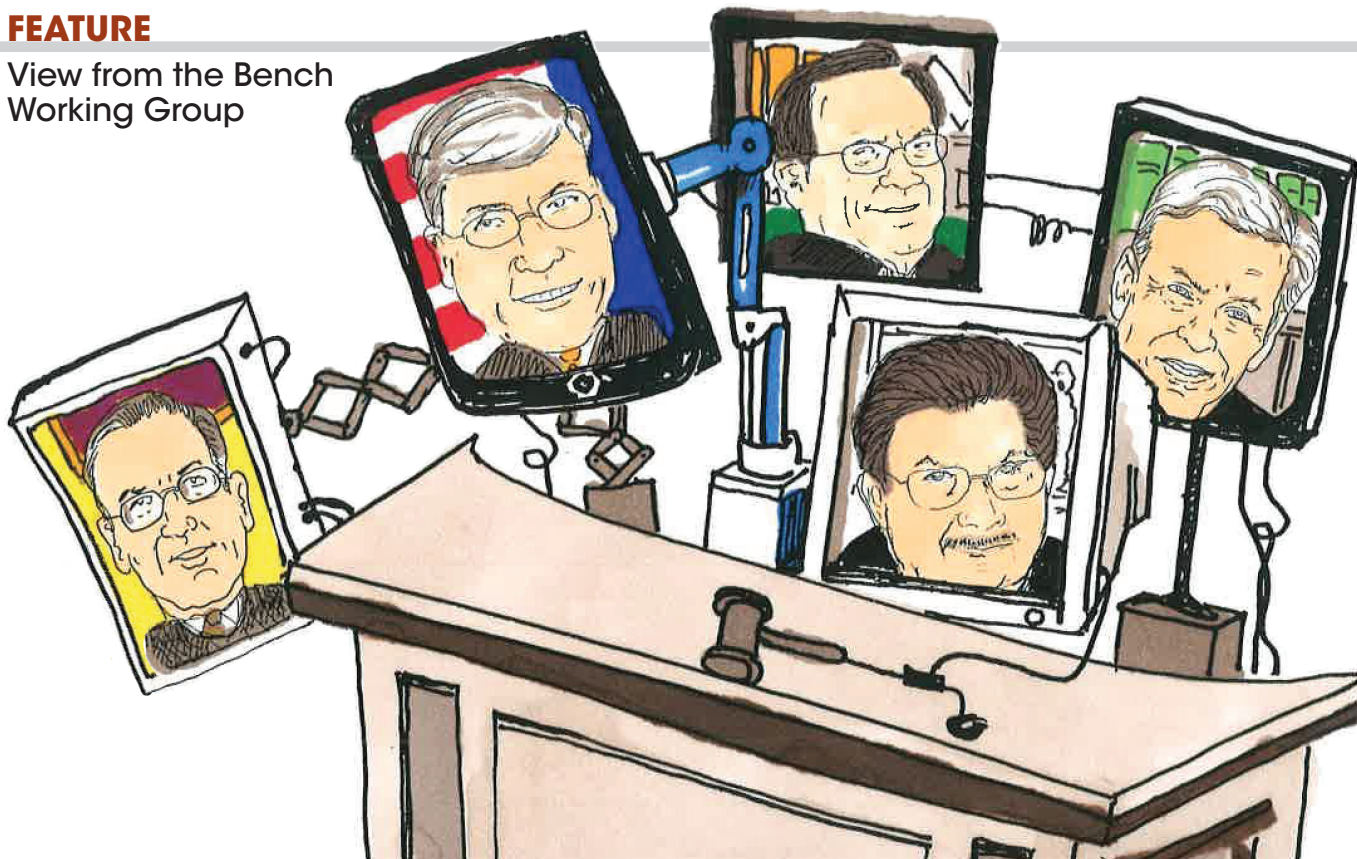
is a director at Prickett, Jones & Elliott, P.A. His practice focuses on litigation involving mergers and acquisitions, corporate governance, and other complex corporate governance and business matters primarily in the Delaware Court of Chancery. Mr. Jameson also regularly acts as counsel to directors and officers of Delaware corporations regarding matters of corporate governance. He is a member of the Rules Committee of the Delaware Court of Chancery, the Corporation Law Section of the Delaware State Bar Association, the Delaware Board of Bar Examiners, and the Delaware Supreme Court Commission on Law & Technology.

### Edward J. McAndrew

is an Assistant United States Attorney in the U.S. Attorney's Office for the District of Delaware. He is the District's Cybercrime Coordinator and National Security Cyber Specialist. Before moving to Delaware in 2008, he was a member of the Cyber Crime Unit of the U.S. Attorney's Office for the Eastern District of Virginia. He previously was a litigation partner in the Washington, D.C., office of Reed Smith LLP. In addition to his government investigations and technology litigation practice, he served as the Deputy Practice Group Leader of Reed Smith's Global Regulatory Enforcement Group. He began his legal career in Wilmington as a law clerk to the Honorable Collins J. Seitz of the United States Court of Appeals for the Third Circuit. He leads the Commission on Law and Technology's Data Security Working Group, and is a frequent presenter and author on issues related to cybercrime, computer forensics, data security, digital privacy and Internet safety.







# “Please Allow [Us] to Introduce Ourselves”:<sup>1</sup> The Commission on Law & Technology

The Honorable  
Henry duPont Ridgely

The Honorable  
Donald F. Parsons, Jr.

The Honorable  
Eric M. Davis

The Honorable  
Michael K. Newell

The Honorable  
Kenneth S. Clark, Jr.

About the time that this edition of *Delaware Lawyer* reaches your desk, tablet, computer or other mobile device, the Commission on Law and Technology (Commission) will have celebrated its one-year anniversary. The Commission was created by an Order of the Delaware Supreme Court on July 1, 2013, which was amended on August 26, 2013 (the Order). The Commission held its inaugural meeting on September 25, 2013, and has met regularly, usually monthly, since then.

The spring 2007 edition of *Delaware Lawyer* was entitled “Silver Celebration – A Look Back – And Ahead – At the Legal Profession in Delaware.”<sup>2</sup> The main article featured a roundtable discussion with lawyers and judges, most of whom were admitted to the practice of law between 1981 and 1983. The participants discussed the changes to the practice of law over the prior 25-year period.

During this lively and no-restraints discussion, the moderator asked the

panel to comment on the effect of technology on the practice of law. The responses, some humorous some serious, were: “It’s the devil’s work”<sup>3</sup>; “It’s a blessing and a curse”; and “It’s the great equalizer” (between small firm/large firm litigation).

While there was discussion that legal research was made easier by technology, one participant posited whether that was a good thing since reading the entire case and not just the highlighted material made one a better lawyer. Of

course, the speed of electronic communication and the expectation of an immediate response were also discussed. This roundtable discussion took place only seven years ago. Coincidentally and appropriately, the same edition contained an article entitled “How Technology Has Changed Our Practice of Law” written by Richard Herrmann, Esquire.

More recently, Chief Justice Strine spoke of how aspects of current technology have had a less-than-positive and appealing effect on the practice of law:<sup>4</sup>

Clients produce more and more information cheaply, demand answers in unreasonable time frames, and do not hesitate to burden lawyers with e-mail and even text questions at all times of the day and with no regard to the concept of a weekend. Correspondent counsel have reacted to e-filing by considering midnight to be the standard time to file NON-expedited papers. These practices endanger law practice on both the qualitative and the human dimension. The qualitative aspect is often overlooked, but clients who demand hasty, instant answers to problems that even a decade ago would have been the subject of a careful, deliberative process among colleagues will get answers that are not well thought out. Likewise, when out-of-state counsel routinely file at crazy times of day, there is a natural tendency for the local lawyers not to be as involved in the final draft as should be the case, leading to poorer products for clients and increasing the possibility that briefs that do not meet Delaware standards of quality slip through for filing.

This article will not explore how technology has impacted the practice of law. We are now working and living in a legal/technology environment. Rather, this article will discuss why the Commission is a necessary and forward-thinking concept and why we, as

---

## A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to the representation of a client.

---

lawyers and judges who practice law in Delaware, will benefit from the Commission.

### Events Prior to Creation of the Commission

In 2009, then-American Bar Association President Carolyn Lamm established the ABA Commission on Ethics 20/20 charged with updating the ABA’s Model Rules of Professional Responsibility. The ABA Commission issued its report in 2012 with attention to “clients and lawyers in a technology driven global economy while protecting the public and our system of justice.”<sup>5</sup> The ABA House of Delegates approved the recommended changes to the Model Rules on August 6, 2012.

On August 28, 2012, the Delaware Supreme Court asked the Permanent Advisory Committee (PAC) on the Delaware Lawyers’ Rules of Professional Conduct (DLRPC or Rules) for its recommendations regarding the ABA Commission’s report.

The PAC submitted its report to the Supreme Court on December 13, 2012.

By Order dated January 15, 2013, the Supreme Court amended the DLRPC effective March 1, 2013.

### Notable Rule Changes

As a result of the Supreme Court’s Order, a number of the Rules were amended to include and/or address technology. Some rules, although unchanged, should be read and under-

stood within the context of technology. The following are some of the more notable changes to the DLRPC.

#### (a) Rule 1.0: Terminology

Rule 1.0(n) defines “writing or written” as a tangible or electronic record of a communication. The rule was amended to specifically include electronic communications, and not just email, as a “writing.”

#### (b) Rule 1.1: Competence

This rule was not changed but the change to Comment 8 was one of the reasons for the formation of the Commission. The comment requires a lawyer to “keep abreast of changes in the law and its practice, including the benefits and risks associated with technology.”

#### (c) Rule 1.4

We have always had a duty to promptly advise our clients of circumstances affecting their case. This rule no longer makes reference to an attorney’s obligation to return phone calls, rather a lawyer “should promptly respond to or acknowledge client communication.” (Questions that come to mind when reading this rule are: “What is prompt? Was it prompt to return a telephone call within 24 hours just a few years ago? What is our expectation for an email or text response?”)

#### (d) Rule 1.6

Remember Comment 8 to Rule 1.1 about the benefits and risk associated with technology? Speaking of such risks, lawyers are urged to undertake a thorough reading and understanding of DLRPC 1.6 regarding confidentiality of information. “A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to the representation of a client.”

Who hasn’t experienced or been embarrassed by the inadvertent email which was sent or forwarded by “replying to all” instead of “reply” or by not paying attention when the addressee was someone other than the intended recipient?

Comment 18 to this rule requires a lawyer to act competently to “safeguard information of a client against unau-

thorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of a client or who are subject to the lawyer's supervision."

A lawyer does not violate the rule if the lawyer has made reasonable efforts to prevent the access or disclosure. The comment sets forth a number of factors in determining the reasonableness of the lawyer's efforts.

Rule 1.6 may be the rule with the most impact on the day-to-day practice of law given the use of technology by lawyers and law firms.

**(e) Rule 4.4**

This rule creates a duty by a lawyer who receives a document or electronically stored information (ESI) that was sent inadvertently to promptly notify the sender.

Comment 2 to Rule 4.4 clarifies that a document or ESI is inadvertently sent when it is "accidentally transmitted by a misaddressed email or letter or document or electronically stored information is accidentally included with information that was intentionally transmitted."

**(f) Rules 5.1 and 5.3**

While DLRPC 5.1 and 5.3 do not expressly reference technology, they do create obligations on the part of partners, managers and supervising attorneys to ensure that their respective firms, lawyers, and/or vendors are conforming to the Rules.

Rule 5.1(c) creates responsibility for another lawyer's violation of a DLRPC if the lawyer orders or has knowledge of the specific conduct or if the lawyer is a partner or has managerial or supervisory authority.

Also, please note the obligations of a law firm or lawyer when outside vendors are hired and/or non-lawyer assistance is provided. Safeguards must be in place to ensure that the non-lawyer's conduct is compatible with the professional obligations of the lawyer. See DLRPC 5.3. See also DLRPC 1.6.

**Enter Messrs. Herrmann and Brady**

So halfway through this article, what do the previous sections have to

**The more technologically savvy attorneys could use guidance in security and ethics while the not-so-tech-competent lawyers need to understand technology.**

do with the Commission? The answer is everything.

Richard Herrmann (Richard) and Kevin Brady (Kevin) are leaders and experts, both locally and nationally, in the area of law and technology. Kevin is also the current President of the Technology Inn, which is named after Richard.

After one of the Technology Inn's monthly meetings during 2013, Richard and Kevin approached Justice Henry duPont Ridgely and Justice Randy Holland with the idea of creating a new arm of the Supreme Court devoted to technology and the practice of law.

On March 13, 2013, Richard and Kevin submitted a written proposal for the establishment of a fourth arm of the Delaware Supreme Court in order to "assist the Supreme Court in providing Delaware Lawyers with sufficient guidance and education in the aspects of technology and the practice of law and to facilitate compliance with the Amended Rules of Professional Responsibility." They were invited to attend an administrative meeting of the Supreme Court to present their idea. The historic meeting was held on March 5, 2013, in Justice Ridgely's Chambers at Eden Hill in Dover.

The main reason offered for the creation of the Commission was to assist in lawyer competency in the area of tech-

nology and the practice of law, keeping in focus the need to maintain privilege and confidentiality.

The proposal suggested that the Commission would address: security issues, metadata, cloud computing, and mobile technology.

At the time of the proposal, two target populations were identified: those who were raised in a digital world and those who were not or, as otherwise stated in a general way, younger and older attorneys, respectively. The more technologically savvy attorneys could use guidance in security and ethics while the not-so-tech-competent lawyers need to understand technology.

The proposal was accepted by the Supreme Court and on July 1, 2013, the Court issued the Order establishing the Commission as of September 15, 2013. The Supreme Court issued a press release on July 10, 2013, announcing the creation of the new arm of Court. Justice Ridgely explained, "Other Supreme Courts throughout the United States are making or considering similar amendments...but Delaware is the first State to create and task a Commission with the responsibility of assisting its lawyers in this regard. We live in an ever changing world of technology, and it is having a direct impact on the way lawyers are practicing law."

**Composition and Rules of the Commission**

According to the Order, the Commission is comprised of "no less than 15 members appointed by the Court for a term of 3 years." At least one attorney or judge will be appointed from the following:

- (a) Large firm (at least 50 attorneys)
- (b) Medium firm (20-50 attorneys)
- (c) Small firm (10-20 attorneys)
- (d) Small firm (1-10 attorneys)
- (e) Corporate counsel from a Delaware Corporation
- (f) Delaware Department of Justice
- (g) Chief Information Officer of a large firm
- (h) Chief Information Officer of a medium firm



*Mahogany & More*

## Office Desks & Conference Tables



## Office Seating, Desk & Guest Chairs



## Files & Bookcases



*Providing the area's largest selection of fine office furniture.  
Guest seating, desk chairs, file cabinets and more.*

## OAKS, PENNSYLVANIA

1620 East Circle Drive • Oaks, PA 19456

**610-666-6500**

**CLOSED TUESDAY • MON, WEDS & THURS 11AM TO 7PM**  
**FRIDAY & SATURDAY 10AM TO 9PM • SUN 11AM TO 6PM**

**WILMINGTON, DE**

5600 Concord Pike • Wilmington, DE 19803

**302-477-0300**

**TUES APPOINTMENT ONLY • MON, WEDS & THURS 10AM TO 8PM**  
**FRIDAY & SATURDAY 10AM TO 8PM • SUN 11AM TO 6PM**

**We Gladly  
Accept...**



[www.mahoganyandmore.com](http://www.mahoganyandmore.com) | [info@mahoganyandmore.com](mailto:info@mahoganyandmore.com) |  [@mahoganyandmore](https://twitter.com/mahoganyandmore)

Sale prices do not apply to previous purchases. Advertised items at cash price plus tax. Limited stock. Furniture photographs for illustration purposes only. EXCLUDES CLEARANCE ITEMS, ADVERTISED ITEMS, SUPER BUYS PACKAGE DEALS & CASH PRICES. \*Bonded leather is 17% leather. †All financing offers with no interest and/or no payments require credit approval, a minimum purchase and a down payment. SEE STORE FOR DETAILS. Sale offer not in conjunction with any previous offers or sales.

- (i) A judge from the Court of Chancery or the Superior Court
- (j) A judge from the Family Court
- (k) A judge from the Court of Common Pleas or the Justice of the Peace Court

The Court also promulgated rules for the Commission. Of significance is the language in Rule 4, which requires the Commission to develop and publish guidelines and best practices. The intent of the guidelines is to assist members of the Delaware Bar and not to create “a threat or risk of any kind. The failure of an attorney to adhere to a published guideline or best practice is not admissible for any purpose in any civil action in any court.”

The Commission is required to create and maintain a knowledge bank of opinions and articles relating to ethical issues involving technology and the practice of law. The knowledge bank is to be available electronically to all members of the Delaware Bar.

In addition to the knowledge bank, the Commission is required to create and present at least four hours of continuing legal ethics approved education each year.

### The Commission at Work

Rule 3 of the Commission requires the Commission to meet quarterly. It was agreed at the very first meeting that the Commission should meet monthly until further notice. Currently there are nine “working groups” of the Commission: Basic Skills, The Cloud, Courtroom Technology, Data Security, eDiscovery, Email, Mobile Technology, Social Media, and a View from the Bench. To date, each working group has published at least one leading practice note. These articles or notes are published on the Delaware Supreme Court Commission on Law and Technology website which can be found on the official website of the Delaware State Courts.

In addition to the leading practices notes, the Commission, in conjunction with the Bifferato Law Forum, co-sponsored two continuing legal education seminars which can be viewed on the

Commission’s website. The first program was held on February 28, 2014, to introduce the Commission, its website, and the first article from the View from the Bench working group. The second presentation focused on mobile technology.

The Commission’s website is also host to a “FAQs” section and the “Technology Minute,” where one can hear the dulcet tone of Richard Hermann recite a recent snippet from a leading practice note or offer a “technology tidbit.”

Attorneys can also submit a question to the Help Desk by using their Bar identification number to log in and complete a form with their questions, ranging on topics from software support, communication tools, and data management to training resources. Since this is not a “live” help desk, responses are usually provided by email within three days of a request.

If you remain unimpressed by the previously mentioned activities, consider the following. Do you recall the furor and consternation over the security bug entitled *Heartbleed*? Well, the Commission promptly published a FAQ on this important topic for members of the Bar.

The Commission has been active and proactive in this perpetually changing technology environment. Monthly meetings are run efficiently and focus on a leading practice group’s presentation. In the time between meetings, there is usually discussion of the technology issue “*du jour*” with an intention to alert, advise and instruct the Bar.

### The Role of the Courts

Each of the Delaware Courts has addressed technology and law in the context of their respective jurisdictions and obligations to the lawyers who appear before them. The Supreme Court has taken the lead by the creation of the Commission as an arm of the Court.

The Court of Chancery has published “Guidelines to Help Lawyers Practicing in the Court of Chancery.” These guidelines include directions on discovery and preservation of ESI.

Likewise, Superior Court President Judge Vaughn issued Administrative Directive No. 2010-3 creating the Complex Commercial Litigation Division (CCLD). The directive calls for a case management order to issue in each case which shall establish procedures for electronic discovery.

The Family Court and the Court of Common Pleas have each sponsored training for their judicial officers on the benefits of technology in achieving justice.

The Courts recognize their duty to stay current with technology and its effects on the law and the judicial process.

### Conclusion

Delaware was the first state to ratify the United States Constitution and is now the first state to have created a Commission on Law and Technology. It is a privilege to practice law in Delaware, and we should appreciate our forward-thinking Supreme Court and the leadership of Richard and Kevin. The Commission was created to assist lawyers in the practice of law in the ever-changing technological environment.

So again we ask: Is the Commission necessary? The articles following will hopefully convince you that it is. Even if you disagree that it is necessary, it is definitely a benefit to the Delaware lawyer. And finally to adapt the words of Mick Jagger: “So if you meet [us], have some courtesy, have some sympathy, and some [faith].”<sup>6</sup> ♦

### FOOTNOTES

1. Deviation of the opening line from ROLLING STONES, SYMPATHY FOR THE DEVIL (ABKCO Records, 1968). Any comparisons between technology and the devil are unintended and purely coincidental.
2. The spring 2007 *Delaware Lawyer* celebrated the 25th anniversary of the magazine.
3. See note 1.
4. State of the Judiciary Address, Chief Justice Leo E. Strine, Jr., 2014 Bench and Bar Conference.
5. ABA Commission on Ethics 20/20 – Introduction and Overview, August 2012.
6. ROLLING STONES, SYMPATHY FOR THE DEVIL (ABKCO Records, 1968). The authors have substituted the words “us” for “me” and “faith” for “taste” from the original lyrics.





# WIDENER LEADERSHIP WORKS FOR VETERANS

**Widener Law Delaware salutes the Veterans Law Clinic, winner of the 2014 Delaware Governor's Outstanding Volunteer Award for Community Service.**

Since 1997, the Veterans Law Clinic has provided free legal aid to thousands of disabled veterans and their dependents. Last year, the clinic represented 302 veterans. Over 17 years, it has recovered more than \$6 million for veterans.

The clinic specializes in cases from throughout the country that are on appeal to the Board of Veterans Appeals and the Court of Appeals for Veterans Claims.

Widener Law Delaware's Veterans Clinic is one of many outstanding programs that attest to our commitment to our community. Last year, our **Wills for Heroes** program was honored with the 2013 Delaware Governor's Outstanding Volunteer Award for Community Service.

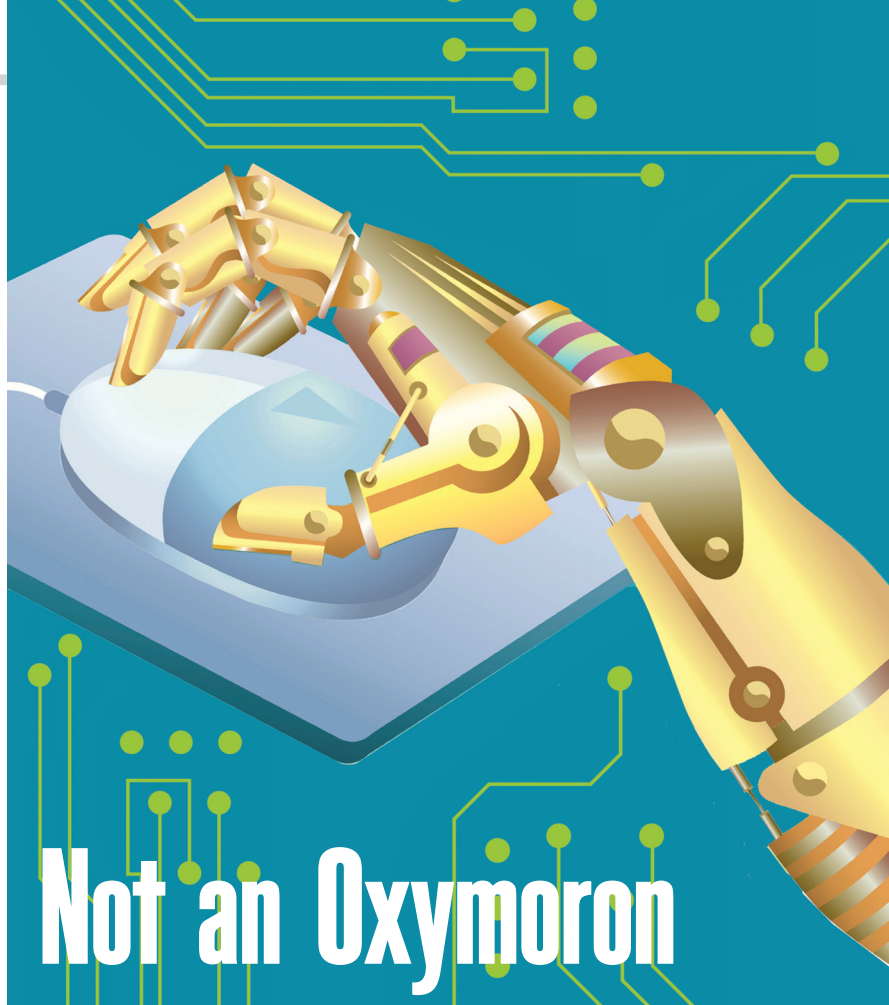
To learn more, visit [law.widener.edu](http://law.widener.edu).

Widener Law



# Technology Competence for Lawyers:

# Not an Oxymoron



A few smart measures — plus some old-fashioned steps like proofreading — can prevent the inadvertent release of confidential information.

“There seems to be some perverse human characteristic that likes to make easy things difficult.”  
— Warren Buffett

I am reminded of this quote when I hear lawyers talking about technology, and particularly the requirements of the Delaware Lawyers’ Rule of Professional Conduct that were adopted on January 15, 2013.<sup>1</sup> But avoiding many problems that lawyers encounter with technology is not complicated.

For example, a lawyer accidentally disclosed confidential information about settlement discussions between her client, Eli Lilly & Co., and the federal government to a *New York Times* reporter. The lawyer mistakenly thought she was sending the email to her co-counsel who had the same last name as the *Times* reporter.

Shortly after receiving the errant email, the *Times* printed a story about those confidential negotiations.<sup>2</sup> The lawyers’ mistake did not result from the technology itself, but rather from failing to proofread the email addresses closely before hitting send.

## Professional Obligations Relating to Technology

In 2013 the Delaware Supreme Court amended the Delaware Lawyers’ Rules of Professional Conduct (“DRPC”) to address the growing relationship between technology and the ethical practice of law. The major technology related amendments include:

- The comments to Rule 1.1 of the DRPC regarding competency now require a lawyer to “keep abreast of changes in the law and its practice, including the benefit and risks associated with relevant technology...”;<sup>3</sup>
- Rule 1.6 and the related comments require a lawyer to make reasonable efforts to address the risks of inadvertent or unauthorized dissemination of information electronically;<sup>4</sup>
- Rules relating to record retention and communications now apply explicitly to electronic records, and to new forms of information that are

unique to electronic records such as metadata (Rules: 1.1 cmt. 9; 1.4 cmt. 4; 4.4(b) and cmt. [2]); and

- Client development and marketing through the internet and electronic communications are specifically addressed in the Rules. (Rules: 1.18; 5.5 cmt. [21]; 7.1 cmt. [3]; 7.2 various cmts; 7.3 cmts. [1] – [3]).

This article focuses on one problem that lawyers often seem to encounter when using technology; the inadvertent and unauthorized dissemination of confidential information.

### **Avoiding Inadvertent Disclosures – The Basics**

Technology in the practice of law has freed lawyers from their physical office by making reliable, instantaneous communication possible from virtually any location. With that freedom and convenience, however, comes an increased risk of accidental disclosures of information. Lawyers need to recognize those increased risks and take steps to minimize them.

#### ***Mobile Device Use in Public***

Technology use in public places increases the risk of inadvertent disclosure of information in multiple ways. In 2009 a Pillsbury Winthrop lawyer was talking loudly on his cell phone on the Amtrak train about coming layoffs at the firm.<sup>3</sup> While the information disclosed related to an internal firm matter, not a client matter, it is easy to imagine how a lawyer discussing a case on a mobile phone in public could inadvertently disclose confidential client information. Simple rule: do not discuss confidential information in public places.

Using mobile computing devices such as laptop computers, tablet computers and smart phones in public locations creates a risk of inadvertent disclosure. People in close proximity to you may see information on your display screen. To reduce that risk, consider use of a privacy screen; a plastic screen placed on your mobile device that prevents viewing the contents of your display screen from side angles. Only a person directly in front of the screen can see its contents. Privacy screens are available for com-

---

## **Lawyers should use only non-public secure WiFi networks, which require a password for access, for confidential communications.**

---

puter monitors, laptop computers, tablet computers, and all types of smart phones and are relatively inexpensive.

Lawyers often use wireless networks, commonly referred to as WiFi networks, to connect their mobile devices to the internet. Many restaurants and stores (Starbucks for example) maintain public WiFi networks. Such public networks should be used with great caution generally and never to transmit confidential information. Transmissions over public WiFi networks can be easily intercepted by strangers.<sup>4</sup>

Lawyers should use only non-public secure WiFi networks, which require a password for access, for confidential communications. If you need WiFi in locations where a secure network does not exist, most major wireless phone companies (Verizon, AT&T, Sprint, T-Mobile) offer users the ability to create their own secure WiFi networks anywhere mobile phone service is available. The user's mobile phone or a "mobile hotspot" device allows the user to create his or her own secure WiFi Network.

#### ***Password Protection***

All computers, tablets and smart phones should be password protected. Not only should you be required to enter a password when the device is first turned on, the device should lock and require a password if the device is not used for a reasonable period of time. The period of inactivity that must pass before the device locks should be short (no more than a few minutes) to minimize

the risk that if the device is lost or stolen, information on it cannot be accessed before the automatic lock activates.

Utilizing automatic lock features and passwords requires the use of reasonably secure passwords. Passwords such as "password" and "123456" do not provide much security. The article referenced in the endnote here contains a list of 25 often-used passwords that you should never use.<sup>5</sup> One study found that most eight-character passwords could generally be cracked by researchers in less than two hours.<sup>6</sup>

The importance of strong passwords is heightened by recent news accounts that lawyers and law firms are becoming the targets of hacker attacks more frequently because law firms are considered "soft targets" that often fail to adopt sufficient security measures.<sup>7</sup>

#### ***Remote Locate and Wipe Features***

Most smart phones and tablets allow you to remotely locate and delete all the information on the device if it is ever lost or stolen. When purchasing a mobile phone or tablet, make sure that it offers this locate/wipe feature. It is generally available on current versions of all of the major mobile devices however it may not be available on older versions of those products.

After acquiring a device with this feature, make sure to set it up. The locate/wipe features will let you locate your phone using another internet-connected computer or device. A friend recently lost his iPhone and using his wife's iPhone was able to track his phone to the sidewalk outside the restaurant where he had lunch several hours earlier. Even if you do not locate your mobile phone or device, you can erase all the information on it remotely.

Some companies also offer locate/wipe products that can be installed on laptop computers. However, for such software to work the computer must be connected to the internet. The better strategy for increased security for laptops is to encrypt your hard drive. Encryption makes the information stored on your computer virtually impossible to read without a password or encryption key.

Detailed information regarding encryption is beyond the scope of this article but readily available on the internet and from technology consultants.

#### **Avoiding Inadvertent Disclosure When Using Email**

Email seems to account for many lawyer woes. The errant Eli-Lily email referenced at the beginning of this paper is a good example. Here are some best practices to avoid similar problems.

##### *Proofread*

The best and most effective means to avoid inadvertent disclosure by email has nothing to do with technology. Slow down and proofread the recipients before you hit send. That is it.

##### *Disable Auto-Complete*

Outlook and most email services offer an “auto-complete” feature that suggests or fills in names from your contact list when you start typing their name in the email “To:” “Cc:” or “Bcc” fields. The feature increases the risk that you will accidentally include an unintended recipient on your email like the Eli-Lily lawyer.

The auto-complete feature can be turned off. Whether the reduced convenience of having to type out all email addresses is worth the reduced risk of mistakes is an individual decision.

##### *Delayed Delivery*

Microsoft Outlook includes a feature called delayed delivery. If you turn on the delayed delivery feature in Microsoft Outlook, your email will not be delivered when you hit “send.” Instead it will be held in an Outlook folder called “Outbox” for a designated period of time before being sent to the recipients.

If you “send” your email and then realize that there was a mistake, there is a brief period of time when you can retrieve the email from the Outbox folder and revise or delete it.

#### **Disable “Send” Keyboard Shortcuts**

Email software like Microsoft Outlook allows you to use keystrokes to send your message rather than clicking on the “send” button on the screen. Depending on the version of Outlook, the key combinations of [Ctrl + Enter] or [Alt + S] send an email message.

---

## Sending a Word document to opposing counsel that contains metadata may unwittingly send language from preliminary drafts.

---

Disable these shortcuts. It is very easy to accidentally hit either key combination when typing thereby prematurely sending a message. Here, a little inconvenience (having to click on the “send” button on the screen) is worth the reduced risk of sending a message before it is final.

##### *Body First; Address Last*

Another way to prevent accidental sending of emails is to draft the body of an email first and add the addresses last. Doing this eliminates the risk of sending the email by accident until it is complete. It also forces you to think more about who should receive the email. Since the substance of the email is final, you can choose addressees with the benefit of knowing the final content of your email.

##### *The Dangers of “Reply All”*

The “reply all” button should be used carefully. If you received a message and want to respond to the sender, check the identity of all the recipients of the email before hitting “reply all.” It is easy to inadvertently send a message intended for the author of the original email to an unintended recipient if such person’s addresses is hidden among multiple recipients included in the “cc” field of the original email.

Also be careful about including persons with adverse interests (e.g. opposing counsel and your client) on the same email. Even if you are careful in your use of the “reply all” button, your clients and co-counsel may not be. Your

client might inadvertently send an email intended for you to opposing counsel. Rather than cc’ing your client, forward a copy of the original email in a separate email.

##### *Use BCC Carefully*

The “bcc” field should be used sparingly if ever. If the bcc recipient decides to “reply all,” his or her presence on the original email will be revealed. On the other side, if you receive an email as a bcc recipient, do not use “reply all” and thereby disclose your presence. I use bcc only to send a copy of certain emails to my own inbox. Instead of sending an email via bcc, send a separate email to the desired recipient that attaches the original email.

##### *Be Aware of Metadata*

Metadata is hidden information contained in electronic documents. For example, in a Microsoft Word document, metadata might include information regarding changes made in that document, who made them and when they were made. This information is not readily visible to the user.

Sending a Word document to opposing counsel that contains metadata may unwittingly send language from preliminary drafts, comments on these drafts or other confidential, privileged information.

The details of metadata are beyond the scope of this article, but lawyers should be aware of its existence and take steps to avoid its disclosure when sharing electronic documents. Products which remove metadata from documents are widely available.

#### **Preventing Theft or Interception of Electronic Information — Basic Protections**

##### *Virus and Malware Protection*

Computer viruses and malware are programs that strangers create and secretly install on your computer which then allow those strangers to access information from your computer or which simply destroy or damage files on your computer. This activity is made possible because computers are now connected to the internet which provides hackers with a potential path into a lawyer’s computer.

Commercial products by makers such



as Norton and McAfee exist to protect against these threats. Lawyers must take steps to protect their computers against viruses and malware.

#### WiFi Security

I discussed public WiFi networks above, but many lawyers set up their own in-office WiFi networks. A WiFi network in a lawyer's office, typically will send its wireless signal beyond the walls of the office. Someone in the street outside the office can detect the WiFi network on their devices, and correspondingly attempt to hack into the network while sitting in their car or other location near your office.

When selecting WiFi equipment make sure that it supports the latest WiFi security features and then make sure that you implement them when setting up your network.

#### Tips and Takeaways to Avoid Technological Missteps

- First, read the Rules. It is hard to comply with your professional obligations, if you do not know what they are. Review the recent amendments

to the Delaware Rules of Professional Responsibility.

- Treat your technology devices like you would confidential documents. Take basic precautions such as password protecting the device to prevent access, restricting the ability of others to view your screen, and implementing measures to protect information if the device is lost or stolen.
- Slow down and think. Just because email allows you to communicate instantaneously does not mean that you should. Set up your email system to minimize the risk of accidentally sending an email or inadvertently including an unintended recipient, think about what you are attaching to an email and whether it might have hidden information, and proofread both what you are sending and the list of persons receiving it before you hit send.

#### To Infinity and Beyond<sup>8</sup>

If you are not convinced that Mr. Buffett's observation applies to the re-

lationship between the professional obligations of lawyers and technology, take heart, there is hope. Numerous jurisdictions in addition to Delaware have now amended their rules of professional conduct to address technology issues. Such amendments are generally based on the American Bar Association Model Rules. As more jurisdictions recognize how changes in technology impact the ethical practice of law, more resources and guidance will become available to assist lawyers who are trying to understand and comply with their professional obligations.

Delaware lawyers are fortunate that the Supreme Court had the foresight to create the Commission on Law & Technology putting Delaware at the leading edge of jurisdictions trying to assist lawyers in dealing with changes occasioned by developments in technology. Take advantage of it. With resources like the Commission, Delaware lawyers have

See **Technology Competence for Lawyers**, continued on page 34.

## CERTIFIED PUBLIC ACCOUNTANTS & ADVISORS COVER & ROSSITER



*Directors Marie Holliday, Geoff Langdon,  
Loretta Manning and Peter Kennedy*

*Providing Complete Tax,  
Audit and Accounting Services  
for Attorneys and Law Firms  
throughout Delaware*



*Find out how we can put our experience to work for you!*

Wilmington • Middletown

www.COVERROSSITER.com  
(302) 656-6632



@CoverRossiter

/CoverRossiter



# Securing Your Mobile Device

Protecting your smartphone — and the records and data it contains — is now one of your professional responsibilities.

Imagine that you are returning from a lunch with a colleague followed by a deposition. When you get back to work, you realize that you left your smartphone at the restaurant. You plan to call the restaurant to determine if your phone was found, but as you open your email on your desktop computer, you notice several email messages from your friends, colleagues and clients.

Your contacts are replying to an email message supposedly sent by you, but that you did not send. The email was eliciting personal information from these individuals. You also have several email alerts indicating that password reset requests were sent for your most-used smartphone apps.

You quickly realize that someone else located your smartphone and used the apps that you installed to obtain your personal information and to access several of your accounts. Although your smartphone had just been left at the restaurant a few hours prior, your personal information, and potentially that of your clients, friends and colleagues has been compromised.

## Leading Practices for Mobile Devices

Luckily, the scenario above is a hypothetical situation. However, with the information that is available on our mobile devices, it is easy to see how a malicious individual could wreak havoc on your life if they find your smartphone and it is not properly secured.

The good news is that securing your device is not that difficult or time consuming. The bad news is that based on the January 15, 2013, amendments to the Rules of Professional Conduct<sup>1</sup>, if you fail to secure your mobile device and the data you store on it, you may face dire consequences.

Rule 1.1 requires that attorneys provide competent representation to a



client.<sup>2</sup> Comment 8 to the amended Rule, notes that to maintain competence, an attorney “should keep abreast of changes in law and its practice, including the benefits and risks associated with relevant technology.”<sup>3</sup> Rule 1.6 requires that an attorney take “reasonable efforts” to prevent unauthorized disclosure of information relating to the representation of a client.<sup>4</sup>

These rules do not indicate the minimum level of knowledge needed to be competent in your use of mobile technology or what is considered as taking “reasonable efforts to prevent access or disclosure” of client data, but it is easy to envision basic guidelines that can help you adhere to your requirements.

### **Password Protect Your Device**

The most important step you can take is password-protecting your device. All smartphones and tablets allow the use of at least some password protection. If you are unsure on how to set a password, just perform an internet search for “password protect” followed by the name of your device. Most likely, you will find both videos and written tutorials on securing your device.

At a minimum, your phone should have at least a four-digit passcode to unlock it. The device should auto-lock after a short period, and a password should be required after your device is locked. Although four-digit passcodes are convenient, adding additional digits to your password exponentially increases the time and effort it would take to crack your password.<sup>5</sup> Most devices even offer an option for a factory reset after 10 unsuccessful login attempts.

The most popular smartphone platforms, Google’s Android and Apple’s iOS, both support these password features. You do not have to install any third-party app, you just have to open your settings, and choose a secure password not shared with others. Avoid commonly used passwords, as studies show that almost 20 percent of people use 1234, 1111, 0000, or 1212 as their four-digit passcode on their smartphone.<sup>6</sup> Using one of the most common passwords is like locking your door, but keeping the key in the lock.

---

**Password protection is essential for your smartphone, but also prepare for the possibility that your password is not as secure as you thought.**

---

### **Encrypt Your Mobile Device**

Encryption puts an extra layer of protection between your data and a malicious user. Having a password is nice, but if your data is not encrypted, others could access it. Data encryption is not foolproof (with enough processing power, basic encryption can be deciphered), but it keeps unsophisticated thieves from easily stealing your data.

If you have an Apple device, encryption is simple. If you have a password on your device, it is encrypted.<sup>7</sup> Nothing else is required.

Android is more difficult. To encrypt your device, you have to have a password, but you must also go into the security settings and choose to encrypt the device.<sup>8</sup> Encryption takes about an hour to complete on Android devices, and you must keep your smartphone plugged in during the process. If your Android device has an SD card, you may have to encrypt the SD card separately.

### **Enable Data-Wiping and Remote Location Service**

Once your device is password-protected and encrypted, you also need a way to remotely locate or wipe the device if it is lost or stolen. Both Android and iOS devices have services available to accomplish this goal.

Apple’s solution is called Find My iPhone and is part of your free iCloud account. When you first set up your iOS device, you are prompted to enable this service. If you decline to set up the ser-

vice initially, Find My iPhone can be enabled in the iCloud settings of your iPhone.<sup>9</sup>

Google has a similar service available for Android devices called Android Device Manager. Android Device Manager is available for Android devices running Android 2.3 or above. You enable Android Device Manager by going into the Google Settings App on your Android device and allowing remote location of the device and remote lock and erase.<sup>10</sup>

Once activated, both of these services allow you to use a web browser or mobile app to locate your device. If your device is off, or has no internet connection, you will be unable to locate it. However, for any device that is currently connected, you will see its location on a map, and can remotely send an audible alert, place it in lost mode, or perform a factory reset.

### **Do Not Store Passwords in Your Apps**

Password protection is essential for your smartphone, but also prepare for the possibility that your password is not as secure as you thought. If your password is compromised, and you routinely remain logged-in to services/apps that contain confidential client data, that data and your accounts could easily be taken over by a nefarious user.

If an app provides you with the option of logging out, do so after every use. Never select the option to save your username or password, and always check apps to see if they provide additional password protection. Use different passwords for your apps than you use to login to your device.

Consider using a third-party email client to access email on your device. Normally, the native email app on Android and iOS stays logged-in at all times. This means that if your smartphone password is bypassed, the malicious user may have access to your entire work email, including your calendar, all your email messages, and your contacts. If you use a third-party app for email, normally there are options to separately password protect just the email app.

By logging out of apps after use, and setting up separate passwords to access the apps with confidential data, you



provide a second layer of protection for your data and make it less likely data will be compromised.

## Current Issues for Mobile Security

With the risk involved in data breaches because of misplaced or stolen mobile devices, manufacturers are working on better solutions to secure devices. Current hot topics include smartphone “kill switches,” biometric passwords, ransomware, and forced software updates to name a few. Recent NSA revelations and Court rulings have focused more attention on securing data on smartphones.

### Smartphone “Kill Switch”

Minnesota recently became the first State to pass legislation that will require that smartphones have anti-theft functionality available in order to be sold in the state.<sup>11</sup> Similar measures have been proposed in California and New York.<sup>12</sup> The purpose is to make the resale of stolen devices more difficult, to decrease the theft of smartphones.

The model for some of the “kill switch” legislation is Apple’s Activation Lock. Activation Lock is available on any iPhone or iPad with iOS 7 or later installed. When you activate Find My iPhone, Activation Lock is enabled.<sup>13</sup> Once enabled, Activation Lock requires your Apple ID and password to erase and reactivate your device, to sign out of iCloud or to disable Find My iPhone. This means that even if a thief steals your device, it cannot be reactivated without your password.<sup>14</sup>

Recent studies have shown a dramatic decrease in theft rates of iPhones since Activation Lock was introduced.<sup>15</sup> With the success of Apple’s Activation Lock, it is likely that other states will require native “kill switches” on all devices, and that manufacturers will voluntarily develop technologies similar to Activation Lock. Since Apple’s service is activated by default, and has to be opted-out of, iPhones are a less attractive target for thieves.<sup>16</sup>

### Alternatives to Passwords

Rather than requiring longer and more complicated passwords, many manufacturers are working at finding new ways for you to authenticate your identity. A 16-digit password may re-

Rather than requiring longer and more complicated passwords, many manufacturers are working at finding new ways for you to authenticate your identity.

sult in a more secure smartphone, but in reality, it is not ideal for re-entering dozens of times per day.

Last year, Apple introduced Touch ID for the iPhone 5s. Touch ID uses your fingerprint to confirm your identity. Once Touch ID is enabled, your fingerprint can unlock your iPhone or allow purchases on the App Store.<sup>17</sup> In iOS 8, developers can integrate Touch ID into their apps for authentication.<sup>18</sup> Samsung and HTC also added fingerprint authentication on some models of their smartphones in 2014.

Google is working on location-based and accessory-based unlocking of your device. In the next version of the Android, you can unlock your device when it recognizes your home WiFi router, or by wearing a Smartwatch you have authenticated with your phone.<sup>19</sup> If you are already using a Smartwatch today, there are apps available that will send an alert to your watch if you move out of range of your phone.<sup>20</sup>

The goal of these new technologies is to secure your device in the least invasive manner to keep you productive. By eliminating frequent password input, you are more likely to use security features. Both Google and Apple are developing methods for segregating work apps from personal apps.<sup>21</sup> This means you can make email secure, while still allowing your children to play Angry Birds on your mobile device.

## Ransomware

While the ability to remotely disable or wipe your mobile device is nice when the device is lost or stolen, malicious users have found methods to use these same features to lock you out of your own device. If your Google or Apple account is compromised, and you have enabled Find My iPhone or Android Device Manager, a third party can use these tools maliciously.

There have been reports where individuals received a prompt on their iPhone that it had been locked and demanding a ransom to unlock it.<sup>22</sup> The malicious user logged into the individual’s iCloud account, activated lock mode, and sent a message demanding money to unlock the device.<sup>23</sup> This same thing is possible using Android Device Manager. The owner of the device is threatened that their device will be erased if they do not provide money.

The easy remedy is to reset your device to factory settings. You would lose any data you do not have backed up from your device, but you could use your device again. The problem is that under Apple’s Activation Lock system, if the malicious user changed your iCloud account password, you cannot reset your device without your iCloud password. If you do not know the password, and cannot recover it, your only option would be to visit an Apple store to have the device reset.<sup>24</sup>

### Mobile Device Software Updates

Anyone with a computer knows that software updates are released frequently. Microsoft issues new updates for Windows machines monthly.<sup>25</sup> Apple frequently releases updates to OS X, and even software vendors like Adobe and Google frequently have urgent software updates to be installed. If you read the release notes for these updates, normally security fixes are included in every update.

Smartphones also have security vulnerabilities that are discovered frequently and require patching. As this occurs, users must have urgent access to the security fixes to protect their data. The problem is that the software updates are not often available to the user in a timely fashion.

Our team of financial professionals is  
here to help keep good going.



**Agents, New York Life Insurance Company, Constitution General Office**  
**2961 Centerville Road, Suite 300, Wilmington, DE 19808**  
**(302) 658-0218**

**Terry L. Wolf, CLU, ChFC**  
**[twolf@ft.newyorklife.com](mailto:twolf@ft.newyorklife.com)**

**Donald T. Fulton, CLU, ChFC**  
**[dtfulton@ft.newyorklife.com](mailto:dtfulton@ft.newyorklife.com)**

**Xavier J. DeCaire**  
**[xdecaire@ft.newyorklife.com](mailto:xdecaire@ft.newyorklife.com)**

Registered Representative offering investments through NYLIFE Securities LLC (Member FINRA/SIPC), A Licensed Insurance Agency.

SMRU496908(Exp.01/11/2015) © 2013 New York Life Insurance Company, 51 Madison Avenue, New York, NY 10010

**Life Insurance. Retirement. Investments.**

**KEEP**

**GOOD**

**GOING**

**NEW  
YORK  
LIFE**



Prior to Apple releasing the iPhone, almost all cell phones received software updates only when approved by the cellular carrier. Cellular carriers had no incentives to provide software enhancements to the end user, and it was common for phones to never be updated during their lifetime.

Apple changed how updates were handled. Apple negotiated the ability to update their devices directly. This allows Apple to quickly release patches for software vulnerabilities soon after they are discovered. The problem is that although Apple has had this ability, other manufacturers have failed to negotiate the same terms.<sup>26</sup>

Google develops the Android OS that is on more than 50% of smartphones sold in the United States,<sup>27</sup> but Google allows hardware manufacturers to customize Android and to add skins to it. Once Google releases an update to the core Android OS, any device manufacturer must then update any customizations and obtain cellular carrier permission before releasing an update. Based on this arrangement, it is common for even the newest Android devices to be running versions of Android released more than a year ago.

Google is aware of this problem and sells phones running the native version of Android directly to consumers. These Nexus and Google Play Edition phones receive updates shortly after they are released by Google.<sup>28</sup> Carrier approval is unnecessary before these devices are updated. The problem: these devices are sold unsubsidized through Google's website and cost several hundred dollars more than buying a phone directly from a cellular carrier.

As an attorney, the security of your device has to be a paramount concern. If a security vulnerability is discovered, your mobile device must be patched as soon as possible to prevent any future compromise of your data. With this in mind, it is recommended to pay close attention to whether your device is running the most recent version of the mobile software available. When purchasing new devices, consider software updates as part of your purchasing decision. If the manufacturer of your phone

**If a security vulnerability is discovered, your mobile device must be patched as soon as possible to prevent any future compromise of your data.**

does not have a good history of timely releasing important software patches, consider purchasing a different device.

### Conclusion

Using a mobile device as part of your practice should allow you to be more effective. Although the scenario at the beginning of the article is the worst-case scenario, the steps you can take to prevent it take minimal time and expertise. Setting a password, encrypting your device, enabling a tracking service, and logging out of apps after you use them, prevent most of the risks discussed.

Smartphones are only becoming more powerful each day, and luckily, manufacturers are realizing the importance of security and working to implement measures in the least invasive manner. Until our smartphones are a chip embedded in our brain, using common sense prevents most security disasters and keeps you compliant with the Rules of Professional Conduct. ♦

### FOOTNOTES

1. Order Amending Rules 1.0, 1.1, 1.4, 1.6, 1.17, 1.18, 4.4, 5.3, 5.5, 7.1, 7.2 and 7.3, Del. Supr., Holland, J. (Jan. 14, 2013).
2. Del. Prof. Cond. R. 1.1.
3. *Id.*
4. Del. Prof. Cond. R. 1.6
5. Yoni Heisler, How to Set Up a Complex Password on Your iOS Device, <http://www.tuaw.com/2014/03/05/how-to-set-up-a-complex-password-on-your-ios-device/> (last visited 8/12/14).

6. DataGenetics, *PIN Analysis*, <http://www.datagenetics.com/blog/september32012/> (last visited 8/12/14).
7. Apple, *iOS: Understanding Data Protection*, <http://support.apple.com/kb/HT4175> (last visited 8/12/14).
8. See Jack Wallen, *Encrypt Your Android Smartphone for Paranoid-level Security*, <http://www.techrepublic.com/article/encrypt-your-android-smartphone-for-paranoid-level-security/> (last visited 8/12/14).
9. For instructions to set up, see Apple, *iCloud: Set Up Find My iPhone*, [http://support.apple.com/kb/PH2697?viewlocale=en\\_US](http://support.apple.com/kb/PH2697?viewlocale=en_US) (last visited 8/12/14).
10. For instructions to set up, see Google, *Android Device Manager*, <https://support.google.com/accounts/answer/3265955?hl=en> (last visited 8/12/14).
11. Sean Hollister, *First Smartphone 'Kill Switch' Law Signed in Minnesota*, <http://www.theverge.com/2014/5/14/5718910/first-smartphone-kill-switch-law-signed-in-minnesota> (last visited 8/12/14).
12. See Noelle Swan, *Minnesota Passes First-In-Nation Smart Phone 'Kill Switch' Law*, <http://www.csmonitor.com/USA/USA-Update/2014/0515/Minnesota-passes-first-in-nation-smart-phone-kill-switch-law-video> (last visited 8/12/14).
13. Apple, *iCloud: Activation Lock*, <http://support.apple.com/kb/PH13695> (last visited 8/12/14).
14. *Id.*
15. See Jordan Crook, *Apple's Activation Lock Brings Down iPhone Theft in Major Cities*, <http://techcrunch.com/2014/06/19/apples-activation-lock-brings-down-iphone-theft-in-major-cities/> (last visited 8/12/14), explaining that when comparing the six months before and after Activation Lock was introduced, iPhone robberies fell 38 percent in San Francisco and 24 percent in London.
16. See *id.*
17. See Apple, *iPhone 5s: About Touch ID Security*, <http://support.apple.com/kb/HT5949> (last visited 8/12/14), for a detailed description of Touch ID.
18. See Chris Smith, *Touch ID Will be Available to Any iOS 8 App*, <http://bgr.com/2014/06/02/ios-8-features-touch-id/> (last visited 8/12/14).
19. See Chuong H Nguyen, *Personal Unlocking Makes Security Simple in Android L*, <http://www.androidcentral.com/personal-unlocking-makes-security-simple> (last visited 8/12/14).
20. See *Pebble Locker*, <http://lukekorth.com/blog/pebble-locker/> (last visited 8/12/14), for details about Pebble Locker for Pebble Smartwatches, and *Wear Aware - Phone Finder*, <https://play.google.com/store/apps/details?id=com.nordicusability.wearaware&hl=en> (last visited 8/12/14), for details about the Wear Aware App for Android Wear Smartwatches.
21. See Google, *KNOX Contribution to Android: Accelerating Android in the Workplace*, <https://www.google.com/pressroom/knox/> (last visited 8/12/14).

See **Securing Your Mobile Device**, continued on page 34.

# WHO CAN YOU DEPEND ON WHEN YOUR CLIENTS ARE INJURED?



*Depend on us to  
get you better faster.*

## GETTING YOUR CLIENTS BETTER FASTER!

### **BOARD-CERTIFIED PHYSICAL MEDICINE, REHABILITATION AND INTERVENTIONAL PAIN MANAGEMENT SPECIALISTS**

A MULTI-SPECIALTY TEAM DEDICATED TO TREATING YOUR CLIENT'S PAIN  
WITH NON-SURGICAL CARE & REHABILITATION

### **ACCEPTING NEW MOTOR VEHICLE & WORKERS' COMPENSATION CASES WORKERS' COMP CERTIFIED**

#### Physical Medicine / Rehabilitation / EMG

Barry L. Bakst, D.O., FAAPMR  
Craig D. Sternberg, M.D., FAAPMR  
Arnold B. Glassman, D.O., FAAPMR  
Anne C. Mack, M.D., FAAPMR  
Stephen M. Beneck, M.D., FAAPMR  
Lyndon B. Cagampan, M.D., FAAPMR

#### Pain Management Counseling

Irene Fisher, Psy.D.

#### Interventional Pain Management

Emmanuel Devotta, M.D.  
Pramod K. Yadhati, M.D.

#### Chiropractic Care

Kristi M. Dillon, D.C.  
Brian S. Baar, D.C.  
Debra Kennedy, D.C.  
Marjorie E. MacKenzie, D.C.  
Adam L. Maday, D.C.  
Scott Schreiber, D.C.  
Mark Farthing, D.C.  
Becky Keeley, D.C.  
Hetal Patel, D.C.  
Ty Harmon, D.C.

#### Interventional Pain Management / PMR / EMG

Rachael Smith, D.O., FAAPMR  
Kartik Swaminathan, M.D., FAAPMR

**Depend on Teamwork for:** Physical medicine & rehabilitation, interventional pain management / injections, EMG, ultra-sound guided joint injections, acupuncture, chiropractic care, rehabilitation therapy, psychology / pain management counseling, massage therapy and QFCEs.

**Depend on Time Saving Solutions:** Centralized communication — we'll keep track of every phase of your client's care. Prompt scheduling — often within 24 hours. Timely response — to your requests for documentation. One call for any record requests.

**Depend on Convenience:** Six convenient locations. Hospital consultations at St. Francis and Kent General. Early morning, lunchtime and early evening appointments. Free, handicapped-accessible parking. Transportation available for auto and work-related injuries. Accessible to public transportation. ONE-STOP CARE!

## **GETTING YOUR CLIENTS BETTER FASTER IS JUST A PHONE CALL AWAY. CALL US TODAY!**

#### Wilmington

2006 Foulk Road  
Wilmington, DE 19810  
302-529-8783

700 Lea Boulevard  
Wilmington, DE 19802  
302-529-8783

#### Newark / Glasgow

87-B Omega Drive  
Newark, DE 19713  
302-733-0980

2600 Glasgow Avenue  
Newark, DE 19702  
302-832-8894

#### Smyrna

29 N. East Street  
Smyrna, DE 19977  
302-389-2225

#### Dover

200 Banning Street  
Dover, DE 19904  
302-730-8848

**TRANSPORTATION AVAILABLE**

# Managing Clients'

# Social-Media Evidence

Failure to preserve social-media content can sabotage your case and result in fines or sanctions.

You represent the plaintiff in a personal-injury suit. Your client seeks damages for injuries sustained as a result of a multiple-vehicle accident. During the client's deposition, she is asked by the lawyer for one of the defendants about her social-media use. The client testifies that she has a Twitter and Facebook account and that she posts to both on a regular basis.

The defense lawyer asks whether the claimant has ever posted about her accident on any of her social-media accounts. "No, never," the claimant responds. "And how about your injuries? Have you ever posted about your injuries on Twitter or Facebook?" the lawyer inquires. "Well, maybe," says the claimant.

You feel mildly nauseous as the defense lawyer pulls out an exhibit and slides it across the table. The claimant grimaces as she reads the paper. You pick up the page and see a screenshot of a Twitter feed. Next to the tweet is your client's tiny picture. The tweet was posted from your client's Twitter account.

The tweet says, "Follow-up appointments are the stupidest thing ever! My

wreck was forever ago! I'm FINE!!!" The defense lawyer launches into a series of questions about the tweet and about other comments your client may have posted to her social-media accounts. Your client admits that she posted the tweet, that she may have posted others like it, and that she has not made any efforts to collect or otherwise preserve online content relating to the accident or her injuries.

At the conclusion of the deposition, the lawyer puts a request on the record, seeking all other relevant social-media content. You dismiss that defendant the following day. And then you thank your lucky stars that nothing worse came out of your failure to preserve your client's social-media content.



## Current Issues

Content posted onto online social-media sites, such as Facebook and Twitter, is subject to the same duty to preserve as other types of electronically stored information, such as email and electronic documents. The duty to preserve is triggered when a party reasonably foresees that evidence may be relevant to issues in litigation. All evidence is a party's "possession, custody, or control" is subject to the duty to preserve.

### *Social Media as Potential Evidence*

Parties in litigation are entitled to discovery of all relevant, non-privileged information. Thus, social-media content is subject to discovery, despite the privacy settings imposed by the user. Nevertheless, the user's right to privacy is commonly an issue in discovery disputes involving social media. Litigants continue to contend that their Facebook content is "private" and should not be subject to discovery during litigation. They argue that privacy protections are available because their Facebook pages are not publicly available but, instead, are available only to a limited number of designated Facebook "friends."

This argument is consistently rejected by courts. Instead, courts find that "private" is not necessarily the same as "not public." By sharing content with others, even in limited numbers, the user has lost his or her right to keep such information "private." The logic is compelling – social media gets its name from the social nature of the medium. If users truly desired to keep the information private, they would not have posted it to a social-media account. Consequently, discoverability of social media is governed by the typical relevancy analysis applied to any other type of evidence and is not subject to any "social-media" or "privacy" privilege.

### *Why Preservation of Social Media Matters*

Due to the broad scope of discovery, lawyers must be diligent in ensuring that all potentially relevant evidence stored on their clients' social-media accounts is preserved for litigation. Failure to properly preserve social-media evidence can result in significant con-

---

## Social-media content is subject to discovery, despite the privacy settings imposed by the user.

---

sequences, including sanctions. And, when it comes to the duty to preserve, ignorance of the client or of the lawyer is not a defense. For example, in *Painter v. Atwood*, No. 2:12-CV-1215 JCM (NJK), 2014 U.S. Dist. LEXIS 98669 (D. Nev. July 21, 2014), the defense sought to compel certain comments and pictures posted to the plaintiff's Facebook page.

When the plaintiff denied that the content existed, the defense produced copies of the pictures and comments, which had been obtained from one of the plaintiff's Facebook friends. The plaintiff admitted that, although the content had once been posted to her account, it had since been deleted, claiming that she "regularly" deleted pictures and posts. The defense moved for sanctions for the plaintiff's failure to preserve relevant evidence.

In response to the motion, the plaintiff's counsel argued that the plaintiff had not understood the duty to preserve because she was a "young girl." The court was not moved. In finding that the plaintiff had spoliated the evidence, the court reasoned that age nor gender were relevant and that, in any event, it was the duty of counsel to instruct her client about the need to preserve.

Although the court determined that spoliation had occurred, it did not order sanctions because the defense had been able to obtain copies of the deleted content. A similar approach was taken in *Katiroll Company, Inc. v. Kati*

*Roll and Platters, Inc.*, No. 10-3620 (GEB) (D.N.J. Aug. 3, 2011). In that case, the court determined that the defendant had committed technical spoliation when he changed his Facebook profile picture, where the picture at issue was alleged to show infringing trade dress. Because the defendant had "control" over his Facebook page, he had the duty to preserve the photo.

The court found that the photo was relevant to the litigation and, therefore, its removal was "somewhat prejudicial" to the plaintiff. Instead of awarding harsh monetary or evidentiary sanctions, though, the court took a more practical approach. Specifically, the court ordered the defendant to change the picture back to the allegedly infringing picture for a brief period of time, thereby enabling the plaintiff to print copies of whatever it believed to be relevant.

Critical to the court's ruling was its finding that the plaintiff had not explicitly requested that the defendant preserve his Facebook account as evidence. Unlike the court in *Painter*, here the court concluded that it would not have been immediately clear to the defendant that changing his Facebook profile picture would constitute the destruction of evidence. Thus, the court found, any spoliation was unintentional.

In *Painter* and *Katiroll*, the courts held that no sanctions were necessary because the defense had been able to obtain copies of the deleted content. But not all courts have adopted this no-harm-no-foul approach. For example, in *Gatto v. United Airlines, Inc.*, No. 10-1090-ES-SCM (D.N.J. Mar. 25, 2013), the plaintiff attempted to deactivate his Facebook account but deleted it instead. As a result, all of the data associated with the account was automatically and permanently deleted 14 days later. The court found that the plaintiff had failed to preserve relevant evidence and ordered an adverse-inference instruction as sanctions.

In *Lester v. Allied Concrete Company*, No. CL08-150 (Va. Cir. Ct. Sept. 1, 2011), *aff'd*, 736 S.E.2d 699, 702 (Va. 2013), the court sanctioned both the

plaintiff and his counsel based, in large part, on its determination that they had engaged in spoliation of social-media evidence. In that case, upon learning that his client had posted less-than-flattering photos to his Facebook page, the lawyer instructed his paralegal to tell the client to “clean up” his Facebook page. The paralegal assisted the plaintiff in deleting 16 pictures from his account and then deactivating his account.

Although all but one of the photos were later recovered by forensic experts, the court found that sanctions were warranted. The plaintiff’s lawyer was ordered to pay \$542,000 in attorney’s fees and was referred to the state bar’s disciplinary counsel, which resulted in an agreed-upon five-year suspension of the attorney’s law license. *In re Matthew B. Murray*, Nos. 11-070-088422 (July 17, 2013).

#### Future Issues

It seems inevitable that parties and their counsel will continue to face the general challenge of complying with the duty to preserve social-media evidence for some time to come. But there are some specific issues that counsel can expect to face in the more immediate future.

One such issue deals with the question of “control.” The duty to preserve applies only to evidence that is in the party’s “possession, custody, or control.” And evidence generally is considered to be within a party’s “control” when the party has the legal authority or practical ability to access it. In the context of online evidence, including social-media content, the concept of control is less obvious than in the context of traditional paper documents or other tangible items.

In the context of online evidence, there is a question of whether an entity “controls” (and, therefore, has a duty to preserve) potentially relevant social-media content of its employees. Although there is not yet a published opinion addressing this question, other recent cases give an indication of how the law may be applied.

For example, in *Cotton v. Costco Wholesale Corp.*, No. 12-2731 (D. Kan.

---

In the context  
of online evidence,  
including social-media  
content, the concept  
of control is less  
obvious than in  
the context of  
traditional paper  
documents or other  
tangible items.

---

July 24, 2013), the plaintiffs, former employees, sought to compel their former employer to produce text messages sent or received by former coworkers. There was no question about the relevancy of the text messages at issue but there was a question about “control” because the messages were sent via the coworkers’ personal cell phones. In denying the plaintiffs’ motion to compel, the court held that there was no basis to find that the employer had any legal right to obtain the text messages. In other words, the court found that the phones and the data they contained were not in the “possession, custody, or control” of the employer.

A different approach was used in *P.R. Telephone Co., Inc. v. San Juan Cable, LLC*, No. 11-2315 (GAG/BJM) (D.P.R. Oct. 7, 2013). There, the court held that the employer *did* have a duty to preserve relevant email from the personal email accounts of three of the company’s former officers. The only facts given by the court as the basis for its decision was that the company “presumably knew” that its officers had used their personal email accounts to conduct company business. The court found that the company had failed to

preserve the emails sent through the officers’ personal accounts.

It would seem that the duty to preserve social-media evidence should not be nearly as difficult when the evidence is within the client’s possession, custody, or control. But many lawyers continue to struggle with the logistics of how to preserve a client’s social-media content. There are several “entry-level” methods to preserve social-media evidence, which require minimal technological knowledge.

Facebook is an excellent example. To obtain all of the content and related metadata from a Facebook account, the user must sign an authorization form, which must be submitted to Facebook, along with a check for \$150. Facebook will then provide all of the data contained in and about the account. This is the most comprehensive method and lawyers should consider having clients execute the authorization form at the outset of the engagement.

But there is a more immediate way to preserve Facebook content, too. After logging into his Facebook account, the user (client) clicks a button called, “Download Your Information.” With just one click, the client will download a zip file containing timeline information, posts, messages, and photos. Information that is not available by merely logging into the account also is included in the zip file, such as the ads on which the user has clicked, IP addresses that are logged when the user accesses his account, and other potentially relevant information. This method offers the lawyer and client the ability to preserve content immediately and without any cost.

Twitter offers a similar, although somewhat limited, option. Twitter users can download all tweets posted to an account by requesting a copy of the user’s Twitter “archive.” Twitter does not offer users a self-serve method of obtaining other, non-public information, such as IP logs. To obtain this additional information, users must request it directly from Twitter by sending an email to [privacy@twitter.com](mailto:privacy@twitter.com) with the subject line, “Request for

Own Account Information.” Twitter will respond to the email with further instructions.

This method does have its limitations, though. For example, it does not provide for content that is posted *after* the user has downloaded his information. But, fear not, new apps are in the works to provide for such collection.

One such app is called Tweet Keeper. Once installed on a user’s smartphone or tablet, the app can be used to download the most recent 3,200 tweets posted from the account. And, once downloaded, the tweets can be filtered, searched, and exported into various formats for use in other applications, such as Microsoft Excel. But perhaps the most unique feature of this particular app is its ability to continue to download new tweets as they are posted to the account, thus resolving the problem of preserving content posted during litigation, after the initial preservation has occurred.

Although these self-help preservation methods can be an excellent start

and certainly are better than taking no steps to preserve, they do not address all possible data associated with a user’s social-media account. There may be some instances when it is advisable to employ the assistance of a third-party vendor in order to ensure complete preservation. Cloud Preservation and X1 Social Discovery are two examples of commercially available tools that are specifically designed for archiving and collecting social-media content. The downside to such tools, of course, is that they come with a price tag significantly larger than Tweet Keeper’s \$1.99 price or even the \$150 Facebook method.

### Conclusion

The unavoidable reality is that social media is here to stay. Consequently, lawyers are well advised to embrace the reality and endeavor to learn the minimal skills necessary to comply with their ethical duties. The good news is that this can be accomplished without the investment of much time or money.

Here are three key things every litigator should remember about social-

media evidence:

- Be aware of its existence. Do not pretend that social-media evidence does not exist. Ask your clients about their social-media usage immediately upon engagement and then throughout the litigation.
- Preserve immediately. Once you know that your client uses social media, take immediate steps to preserve any and all potentially relevant content.
- Preserve more, not less. What may be relevant in any particular case can be an incredibly complex question. The safer practice, by far, is to preserve more than you need, rather than less.

The duty to preserve is a serious one and is no less serious in the context of social media. Although social media may be an unfamiliar source of evidence, it is a critical one. Thus, lawyers should acknowledge the reality and work towards development of a level of familiarity that satisfies the ethical duty of competence. ♦

## Delaware’s Premier Litigation Support Team



Stephen M. Conyers, CPA      Edward P. Byrnes  
Stacey A. Powell, CPA, CFE, CICA      William A. Santora, CPA



**Santora CPA Group**  
*Right, By Your Side*

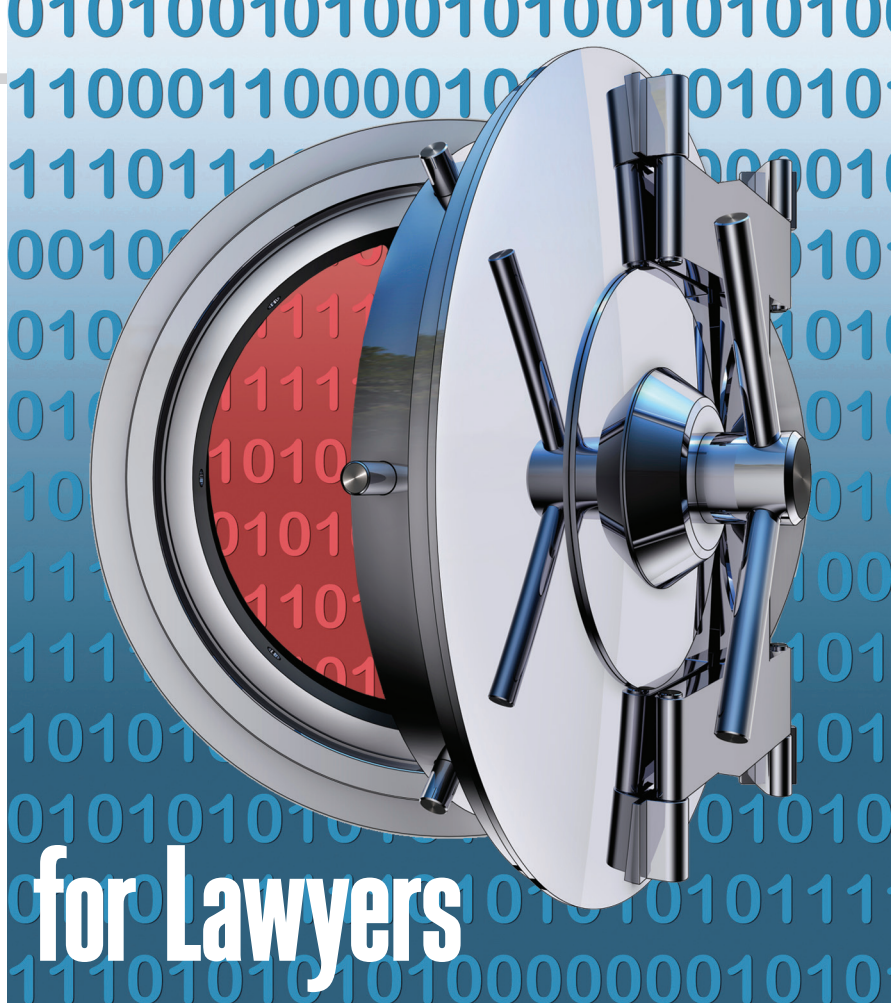
Call 302-737-6200 or toll free 800-347-0116

- Review & Analysis of Documents
- Damage Calculation
- Detailed Expert Report Preparation
- Deposition & Court Testimony
- Rebuttal Reports
- Forensic Accounting





# The Data Security Imperative for Lawyers



With lawyers  
top targets for  
cyberattacks and both  
firm and client data  
subject to loss or  
breach, smart  
security protocols  
are essential.

A small law firm is victimized by ransomware encrypting all data on its network. An international law firm is targeted for cyber espionage by a foreign intelligence service. A law firm's network administrator reads attorney emails to obtain material, non-public information that he then uses for stock transactions. A departing employee downloads highly confidential and proprietary data onto USB drives and uploads it to cloud accounts. Hacktivists breach the network of an investigative firm and upload the firm's emails with lawyers on sensitive projects to a public website. A lawyer loses a smart phone containing unencrypted emails and text messages with a client.

**T**hese are just some of the types of data security and privacy threats that lawyers now face.

## Overview of the Threat Landscape

Data security and privacy have become watchwords of the early 21st Century – for good reason. Digital devices, networks and services collect the details of virtually every aspect of our personal and professional lives. As the Supreme Court recently noted, the search of a mobile phone “would typically expose... far more information than the most exhaustive search of a house.”<sup>1</sup>

The warp-speed adaptation of digital technology has created great challenges to data security and digital privacy. The U.S. intelligence and law enforcement communities have ranked cybercrime as our top national security threat – higher than terrorism or espionage.<sup>2</sup> There is a daily stream of news about hacking: cyber espionage, digital theft of consumer data, money and intellectual property, lost devices exposing private information, and disruption or destruction of digital infrastructure. Nearly half of the adult U.S. population was hacked in the past 12 months.<sup>3</sup>

Cisco's 2014 Annual Security Report aptly stated: "Odds are high that targeted attacks have already infiltrated your networks."<sup>4</sup> Cisco's security software alone blocks 4.5 billion malicious emails and 50,000 network intrusions each day. Most data breaches are never publicly disclosed.

Lawyers and legal services organizations have become significant targets for cyberattacks. Since at least 2009, the FBI has repeatedly issued warnings that hackers are targeting law firms to steal confidential information. In early 2013, a prominent cybersecurity firm estimated that 80 of the 100 largest U.S. law firms suffered data breaches in 2011 alone.<sup>5</sup>

This should not be surprising. Lawyers and legal services organizations are significant aggregators of sensitive data – about themselves, their clients, and their adversaries or counterparts. Like everyone else, lawyers use digital devices to create, transmit and possess data about their own professional and personal activities, and those with whom they come into contact. Legal services organizations interconnect digitally with clients for practice purposes and with vendors for various purposes – including IT services, building operations (HVAC, security, etc.), client account management, procurement, financial services and human resources.

At risk is the data about lawyers and their organizations, as well as access points to their networks through their clients and business partners. Also at risk is the sensitive, often confidential, client-related data contained in the devices and networks of lawyers and those who assist them. Lawyers also receive sensitive and confidential information from non-clients during litigation transactions, and other matters.

This is not just a problem for large organizations. Symantec reported that 31 percent of the cyberattacks it tracked targeted small and medium-sized businesses with fewer than 250 employees, while 50% of all attacks were aimed at businesses with less than 2,500 employees. Nor is every incident malicious. Nearly 30 percent of the data breaches examined by Symantec involved the ac-

cidental loss of digital devices resulting in the exposure of sensitive data.

External cyber actors are far from the only concern. As Edward Snowden has so aptly demonstrated, insiders can simply copy and carry data out of facilities. Users accidentally lose devices containing sensitive data on a daily basis. Even where outside hackers are involved, an authorized user often unintentionally provides them with network access by clicking on hyperlinks or attachments in spear-phishing emails and text messages or by visiting legitimate, but malware-infected, websites.

### **Ethical Obligations Concerning Client Data Security and Privacy**

In August 2012, the American Bar Association issued a report and resolution urging lawyers to use best practices to protect client data from internal and external threat actors. It also amended the Model Rules of Professional Conduct to address technological issues in the practice of law. In January 2013, the Supreme Court of Delaware amended the Delaware Lawyer's Rules of Professional Conduct to track some of the ABA's changes to the Model Rules. Pertinent changes include those listed below.

**Rule 1.1 – Competence** – Part of a lawyer's duty to provide "competent representation" requires "keeping abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology."<sup>6</sup>

**Rule 1.6(c) – Confidentiality** – This new subsection requires lawyers to make "reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."<sup>7</sup>

Comment 19 explains that an inadvertent or unauthorized disclosure of confidential information "does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure."<sup>8</sup> The comment lists various factors relevant to this 'reasonableness' determination, "including, but [ ] not limited to, the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employ-

ing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use)."<sup>9</sup>

Regarding client-related, electronic communications, Comment 20 states that "the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients."<sup>10</sup> A lawyer need not employ "special security measures if the method of communication affords a reasonable expectation of privacy."<sup>11</sup> The sensitivity of the information and the extent to which "the privacy of the communication is protected by law or by a confidentiality agreement" are relevant factors.<sup>12</sup>

**Rules 5.1 & 5.3 – Supervision** – A lawyer must make "reasonable efforts" to ensure that lawyers and non-lawyers working under the lawyer's supervision, management or control comply with all ethical rules.<sup>13</sup> Comment 3 specifically references outside services, which may include investigative and paraprofessional services, document and data management vendors, and cloud services providers. Factors relevant to the reasonableness of a lawyer's efforts include "the education, experience and reputation of the non-lawyer; the nature of the services involved; the terms of any arrangements concerning the protection of client information; and the legal and ethical environments of the jurisdictions in which the services will be performed, particularly with regard to confidentiality."<sup>14</sup>

Comment 19 to Rule 1.6(c) also extends a lawyer's data security duty to supervising "other persons who are participating in the representation of the client."<sup>15</sup>

Other rules relating to communication with clients (Rule 1.4) and duties to prospective and former clients (Rules 1.9 and 1.18) also are implicated in the data security and privacy context. Rule 1.4's duty to "keep the client reasonably informed" and to "promptly comply with reasonable requests for information" may encompass the lawyer's data

security policies and practices. It also may require a lawyer to inform clients of cyber incidents impacting the attorney-client relationship.<sup>16</sup> Rules 1.9 and 1.18 may require a lawyer to maintain the privacy and security of data relating to former or prospective clients.<sup>17</sup>

## Data Security Leading Practices

Based on the evolving cyber threat landscape and the ethical duties summarized above, each lawyer must be actively involved in data security efforts on an ongoing basis.<sup>18</sup> Although cybersecurity is a relatively new responsibility for lawyers, it does not need to be an overwhelming one. Each lawyer is simply expected to act reasonably under the circumstances in an effort to protect the privacy and security of client data.

The Commission on Law and Technology recently published “Leading Practices: Data Security” on its website to assist lawyers in meeting this obligation.<sup>19</sup> The Leading Practices are drawn from a variety of sources that have been widely adopted across public and private sectors. They therefore may have the added benefit of already having been adopted by some clients, with (hopefully) many more to follow as data security and privacy practices take root across broader segments of society.

There is no single, correct way to mitigate cyber risk. Nor is there a single checklist to be mechanically applied to each legal practice. The Leading Practices offer suggestions that can be adapted to fit any individual practitioner or organization. Not every Leading Practice will apply to every lawyer. What makes sense for the largest firms with IT departments may not be necessary, or even appropriate, for the solo practitioner or small firm lawyer. There is, however, a general approach to data security that can be used by all lawyers. That general approach and some basic cybersecurity concepts are discussed below. For a more comprehensive discussion, please visit the Commission’s website at <http://courts.delaware.gov/declt/datasecurity.stm>.

## Core Concepts and the Basics

Like the cyber threats we face, the task of data security is continuous and dynamic. Below are some basic steps to

data security:<sup>20</sup>

- Identify the data, systems and devices to be secured and the threats to them.
- Determine how those threats could impact the lawyer, the organization, clients and others.
- Use the foregoing information to develop a data security plan that fits each lawyer’s (or organization’s) risk profile, goals, budget, legal and ethical obligations. Educate and train all users on the plan.
- Implement and monitor the effectiveness of the data security plan.
- Create a cyber incident response plan for data breaches and other cyber incidents (system crashes, destruction of data, etc.) that might impact a practice. Educate and train all incident responders on the plan.
- Adjust both plans as variables change.

Cyber incidents cannot be entirely eliminated. Many of them can be mitigated, though, by employing basic cyber hygiene and security measures. Summarized below are some of these measures, categorized by how lawyers most commonly create, store and transmit sensitive data.

### Devices and Networks

Secure computers, mobile phones, tablets, USB and other portable drives, digital media and all devices that connect to the network with strong passwords and encryption. Prohibit the sharing of devices. Require that any USB drive or other portable media be encrypted before they may be used. Continually update and patch software and browser vulnerabilities. Employ capabilities to remotely lock, locate and erase data from any mobile device that connects to the network.

Avoid using public Wi-Fi networks to access confidential and sensitive client information. Instead use private, encrypted hotspots or virtual private networks to access such information. Require multi-factor authentication to access networks and online accounts. Limit remote access privileges to essential users.

There are many additional considerations for networks. Listed here are just a few that should be used for even basic networks. Allow only known users and devices with approved configurations to

access a network, and monitor that access/use. Utilize and continually update firewalls and anti-virus, anti-spam, anti-spyware, malware and phishing defenses for networks. Protect confidential and sensitive data with appropriate encryption technology. Restrict access to sensitive information or network areas on a “need-to-know” basis. Tightly control the use of network administrative and other broad-access privileges. Engage in the continuous monitoring of IT systems, networks, security status and risks. Disable any unnecessary or unused accounts. Monitor and control remote access from all endpoints, including mobile devices.

### *Electronic Communications (Email, Text, Instant and Voice Messaging)*

Encrypt communications that contain confidential client information. Transmit decryption keys/passwords via separate communication. Do not transmit confidential client information to personal accounts. Consider transmitting highly sensitive client information through a secure file transfer protocol (FTP) or file sharing service. Do not access confidential client information from shared or untrustworthy devices.

### *Cloud Services Security*

Establish a policy on whether and which cloud services may be used and what data may be stored in those services. Many file hosting programs and applications, such as Dropbox and SkyDrive, are public repositories of data. Confidential and sensitive client information generally should not be stored in such public repositories without strong encryption. Ensure that cloud providers: (1) have no ownership or security interest in data stored in the cloud; and (2) have an enforceable obligation and have taken reasonable steps to secure that data. Be able to obtain all stored data on demand. Know where the data is physically being stored, and comply with all applicable security and privacy laws.

### *Data Retention, Recovery and Destruction*

Perform complete and frequent backups of critical systems, data and devices, with appropriate encryption employed. Have a backup plan in case data stored in a cloud becomes inaccessible. Employ



remote wiping or deletion capability for lost mobile devices, laptops, tablets and other portable digital media. Develop data retention and destruction plans that include protocols for the removal and destruction of all confidential and sensitive data prior to disposal of all devices. Keep only that data that is needed or is required to be kept.

### The Way Forward

Taking reasonable steps to protect client information is nothing new. Confidentiality has always been the keystone of the attorney-client relationship, and we have been using digital technology to practice law for decades. What has changed is the threat landscape, and it will continue to do so.

Cyber threats, and the magnified and deleterious consequences they can bring, require each of us to incorporate digital data security into our practices. We need to educate ourselves and each other about these new threats and develop plans for addressing them. The data security imperative now arises daily, can be daunting, but is doable. ♦

### FOOTNOTES

1. *Riley v. California*, 134 S. Ct. 2473, 2491 (2014).
2. Director of National Intelligence, "Worldwide Threat Assessment of the U.S. Intelligence Community" (Jan. 29, 2014) (prepared statement before Senate Select Committee on Intelligence), *available at* <http://www.dni.gov/index.php/newsroom/testimonies/203-congressional-testimonies-2014/1005-statement-for-the-record-worldwide-threat-assessment-of-the-us-intelligence-community>; Greg Miller, "FBI Director Warns of Cyberattacks; Other Security Chiefs Say Terrorism Threat Has Altered," WASH. POST (Nov. 14, 2013), *available at* [http://www.washingtonpost.com/world/national-security/fbi-director-warns-of-cyberattacks-other-security-chiefs-say-terrorism-threat-has-altered/2013/11/14/24f1b27a-4d53-11e3-9890-a1e0997fb0c0\\_story.html?hpid=hp\\_hp-top-table-main-cyber-security:homepage-link-story&hpid=hp\\_hp-top-table-main-cyber-security:homepage-link-story](http://www.washingtonpost.com/world/national-security/fbi-director-warns-of-cyberattacks-other-security-chiefs-say-terrorism-threat-has-altered/2013/11/14/24f1b27a-4d53-11e3-9890-a1e0997fb0c0_story.html?hpid=hp_hp-top-table-main-cyber-security:homepage-link-story&hpid=hp_hp-top-table-main-cyber-security:homepage-link-story).
3. *See, e.g.*, Jose Pagliery, "Half of American Adults Hacked this Year," *available at*: <http://money.cnn.com/2014/05/28/technology/security/hack-data-breach/>.
4. CISCO 2014 Annual Security Report, *available at*: <https://www.cisco.com/web/offers/lp/2014-annual-security-report/index.html?keycode=000350063>.
5. MANDIANT INTELLIGENCE CENTER REPORT, APT 1: EXPOSING ONE OF CHINA'S CYBER ESPIONAGE UNITS 20, *available at*: [http://intelreport.mandiant.com/Mandiant\\_APT1\\_Report.pdf](http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf).
6. DEL. RULES PROF'L CONDUCT R. 1.1 cmt. 8 (2013).
7. *Id.* R. 1.6(c).
8. *Id.* R. 1.6(c) cmt. 19.
9. *Id.*
10. *Id.* R. 1.6(c) cmt. 20.
11. *Id.*
12. *Id.*
13. *Id.* R. 5.1, 5.3 cmts. 3 & 4.
14. *Id.* R. 5.3 cmt. 3.
15. *Id.* R. 1.6(c) cmt. 19 (citing DEL. RULES PROF'L CONDUCT 1.1, 5.1, 5.3).
16. *Id.* R. 1.4(a)(2)-(4).
17. DEL. RULES PROF'L CONDUCT 1.9, 1.18.
18. THE ABA CYBERSECURITY HANDBOOK 4 (2013). This book is an excellent resource that summarizes many of the legal and ethical data security and privacy standards applicable to lawyers. It also provides suggested approaches to data security for lawyers practicing in different settings.
19. Delaware Supreme Court Commission on Law & Technology Website, *available at*: <http://courts.delaware.gov/declt/datasecurity.stm>.
20. Specific steps to formulating data security and incident response plans, as well as suggested technical components of a data security plan, can be found on the Commission's website, at <http://courts.delaware.gov/declt/datasecurity.stm>.

## GET READY FOR A WINNING COMBINATION.

**Mailboxes • Packing & Shipping • Printing**

Check out everything we do at The UPS Store®. We offer services that make life easier and help keep businesses running smoothly.

4023 Kennett Pike  
Wilmington, DE 19807  
302-429-9780  
store1391@theupsstore.com  
www.theupsstorelocal/1391.com

**Hours:**  
Mon-Fri 7:30 a.m.-7:00 p.m.  
Sat 9:00 a.m.-4:00 p.m.  
Sun Closed



**The UPS Store**



**WE ♥ LOGISTICS™**

## Technology Competence for Lawyers (Continued from page 19)

tools available to take their practices to infinity and beyond through the ethical use of technology. ♦

### FOOTNOTES

1. Delaware Supreme Court by Order dated January 15, 2013, available at <http://courts.delaware.gov/rules/dlrpc2013rulechange.pdf>. See also, the related report of the Permanent

Advisory Committee at <http://courts.delaware.gov/odc/docs/ReportPermAdvComm.pdf>.

2. Debra Cassens Weiss, Did Lawyer's Email Goof Land \$1B Settlement on NYT's Front Page? ABA J., Feb. 6, 2008.

3. <http://abovethelaw.com/2009/02/a-funny-thing-happened-on-the-way-to-new-yorkor-pillsbury-associates-brace-yourself/>

4. See: <http://www.lifelock.com/media/video.php?video=wifi-sniffing>.

5. <http://splashdata.com/press/worstpasswords2013.htm>.

6. <http://www.cnn.com/2010/TECH/innovation/08/20/super.passwords/>.

7. <http://blogs.wsj.com/law/2012/06/25/dont-click-on-that-link-client-secrets-at-risk-as-hackers-target-law-firms/>; <http://apps.americanbar.org/litigation/committees/womanadvocate/articles/summer2013-0813-hackers-are-targeting.html>.

8. Buzz Lightyear.

## Securing Your Mobile Device (Continued from page 24)

<http://android-developers.blogspot.com/2014/07/knox-contribution-to-android.html> (last visited 8/12/14), for details on how Google is using KNOX technology developed by Samsung to segregate personal data from work data in Android L, and see Jesus Vigo, 10 Enterprise Features in iOS 8, <http://www.techrepublic.com/article/10-enterprise-features-in-ios-8/> (last visited 8/12/14), for a description of new management tools for iOS 8 that enable administrators to better manage apps and data on employee devices.

22. Abigail Wang, Ransomware on Apple's iCloud: How the Attack Worked, <http://securitywatch.pcmag.com/security/324170-ransomware-on-apple-s-icloud-how-the-attack>

worked (last visited 8/12/14).

23. *Id.*

24. See Apple, iCloud: Find My iPhone Activation Lock in iOS 7, <http://support.apple.com/kb/HT5818> (last visited 8/12/14), for instructions on using Activation Lock and resetting your device.

25. Microsoft releases updates so frequently, that the term "Patch Tuesday" has been coined for the second and fourth Tuesday of each month when Microsoft usually releases their updates. See Wikipedia, Patch Tuesday, [http://en.wikipedia.org/wiki/Patch\\_Tuesday](http://en.wikipedia.org/wiki/Patch_Tuesday) (last visited 8/12/14).

26. See How-To-Geek, Why Do Carriers Delay

Updates for Android But Not iPhone, <http://www.howtogeek.com/163958/why-do-carriers-delay-updates-for-android-but-not-iphone/> (last visited 8/12/14), for description of the Smartphone update practices.

27. See Jacob Siegal, Despite iPhone 6 Hype, Android Continues to Dominate iOS Market Share, <http://bgr.com/2014/07/01/android-market-share-2014/> (last visited 8/12/14), which indicates that Android is now on 61.9% of smartphones sold in the United States.

28. See Google, Android Updates: Nexus & Google Play Edition Devices, <https://support.google.com/playedition/answer/4457705?hl=en> (last visited 8/12/14).

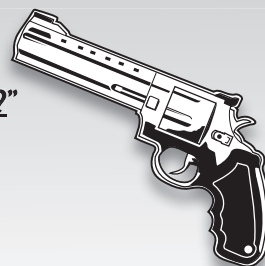


# FIREARMS?

When the question arises, "What do we do with the guns?"  
ARTEMIS OUTFITTERS is your solution.

We offer the following services:

- Estate Sales, consignments, liquidations and dispositions
- Appraisals and evaluations
- Storage (local safekeeping). Prohibited persons, Estate Administration, probate, divorce or PFA orders
- Cleaning, repair, restoration and advice
- We also work with sporting art and collectible decoys



We are a full service dealer experienced with all types of firearms, whether it be one gun or an entire collection.  
Our trained professionals are experienced, friendly and knowledgeable.

*We are a fully licensed and insured Federal Firearms Licensee (FFL).*

One Greenville Crossing | 4021E Kennett Pike | Greenville De 19807  
Tel. 302.384.6861 | [www.artemisoutfitters.com](http://www.artemisoutfitters.com) | [info@artemisoutfitters.com](mailto:info@artemisoutfitters.com)



# DELAWARE BUSINESS TIMES

A division of **todaymedia**

Your local source for essential news,  
information, trends and insights important  
to Delaware businesses.

Every issue of the  
**DELAWARE BUSINESS TIMES**  
will offer insightful coverage of hot  
topics in the Delaware business  
community from north to south:

- News, covering what's "hot," urgent, notable
- Perspective & Trends, creating "the context"
- People, covering the "mover-shaker" Delawareans who are "the moving parts"
- Commentary, Leadership & Advocacy
- In Person & Digital Engagement, Business Leader Events & Round Tables



From the publisher of  
**DelawareToday®**

For Advertising Information: Charlie Tomlinson | 302.504.1335 | [CTomlinson@DelawareBusinessTimes.com](mailto:CTomlinson@DelawareBusinessTimes.com)  
For Subscription Information, visit [www.DelawareBusinessTimes.com/subscribe](http://www.DelawareBusinessTimes.com/subscribe)



# OF COUNSEL: Justice Henry duPont Ridgely

**F**or more than 25 years, Justice Henry duPont Ridgely has been the driving force behind most of the technological changes in the Delaware court system.

He has also been a driving force in educating young people about the judicial process. His lengthy bio lists him as a charter member of many things. One of those things is “the Miracle Team.” This group within the Bench and Bar has provided the opportunity for more than 15,000 children to participate in a live hearing in a courtroom – a hearing that just happens to be the courtroom scene from 20th Century Fox’s *Miracle on 34th Street*.

For the last decade, Justice Ridgely has played a pivotal role in delighting the young citizens of this Great State by ruling “Santa Claus does indeed exist,” after thousands of letters are dumped before him on the bench. He has passed that role onto Judge Vaughn as his way of institutionalizing the event. And now on to more mundane things. . . .

## What You Already Know

Justice Henry duPont Ridgely has served as Justice on the Delaware Supreme Court since his appointment by Governor Ruth Ann Minner on July 22, 2004. Prior to that appointment, he served on the Delaware Superior Court from 1984, and as President Judge from 1990.

## What You May Know

Justice Ridgely received his B.S. in Business Administration from Syracuse University in 1971, his J.D. from The Catholic University of America Columbus School of Law in 1973, and his LL.M. in Corporation Law from George Washington University Law School in 1974.

## What You May Not Know

Justice Ridgely has lead the Delaware Bench and Bar with distinction in his efforts to make us “The First State” when it comes to technology.

In 1991 as President Judge of the Superior Court, he chaired the Superior Court Complex Litigation Task Force, charged with managing the massive environmental insurance coverage litigations paralyzing the Office of the Prothonotary. Docket Sheets of 25 entries in the ordinary personal injury case exploded to thousands in complex cases; each entry needed to be docketed by the clerk’s office. As a result of his forward thinking and leadership, the Task Force created the “First” electronic filing system in the world, now known as File and Serve.

As part of the electronic filing effort, Justice Ridgely was



responsible for the adoption of Superior Court Civil Rule 79.1, which included subparagraph (g), providing that authorization of e-Filing shall constitute a signature under Superior Court Civil Rule 11.

In 2000 he called for the drafting of Superior Court Civil Rule 107(h) permitting the filing of CD ROM briefs.

Once electronic filing became mature in the Superior Court, in 2005, Justice Ridgely now led the Supreme Court to become the “First” appellate court in the nation to implement electronic filing of appeals.

He has served as the Chair of the Delaware Supreme Court’s e-Filing Committee and also as the Co-Chair of the ABA Judicial Division’s Court Technology Committee. Justice Ridgely also has Chaired the Delaware Court’s Automation Project.

Justice Ridgely is a longtime supporter of the ideals of American Inns of Court movement in Delaware. He was President of the Terry-Carey Inn of Court from 1996-98 and in 2009 Justice Ridgely became a Charter Member of the Richard K. Herrmann Technology Inn of Court.

In 2013, his interest in professionalism, ethics and civility lead him to champion a proposal for the creation of a “First” in the nation, Arm of Court, “The Commission on Law and Technology.” The American Bar Association had recently changed the commentary to the Model Rules of Professional Conduct to emphasize the need to be competent in the use of technology in the law. Justice Ridgely had the vision to see that there was a need for guidance for lawyers and judges in this important area. He saw the value of a Commission to develop and publish guidelines and best practices regarding the use of technology and the practice of law.

As Liaison Justice to the new Arm of Court, he said: “We have established a Commission on Law and Technology with broad representation including judges from a variety of Delaware courts as well as lawyers in private practice from various sized law firms, the Department of Justice, in-house corporate counsel and information technology officers.” The Commission has been very active and its work has resulted in information found within the pages of this publication.

In short, Justice Ridgely is “The Distinguished Leader” when one thinks of the mark he has made on the growth of technology in the Delaware legal community through his forward-thinking vision and leadership. ♦



# Foundation.

At Ursuline, we encourage a joy of learning. We build self-confidence. We teach values. And we help your children recognize their connection to a larger world. **Come visit us and see for yourself!**



**Ursuline Academy**  
Growth. Values. For Life.

Educating boys age 3 through grade 5  
and girls age 3 through grade 12

[www.ursuline.org](http://www.ursuline.org) | 302.658.7158



# AN ICON JUST GOT LARGER



THE NEW NAVITIMER 46 mm

SIDNEY THOMAS  
FROM ROSS-SIMONS

Christiana Mall 302.369.3255